PLAN DE RECUPERACIÓN DE DESASTRES DEL SISTEMA DE INFORMACIÓN SERVINTE PARA EL HOSPITAL MÉDERI SEDE PRINCIPAL Y LA SEDE EN BARRIOS UNIDOS

Ing. DIDIER JAVIER HENAO DIXZ
Ing. SANDRA PATRICIA JUNCO ROMERO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

PLAN DE RECUPERACIÓN DE DESASTRES DEL SISTEMA DE INFORMACIÓN SERVINTE PARA EL HOSPITAL MÉDERI SEDE PRINCIPAL Y LA SEDE EN BARRIOS UNIDOS

Ing. DIDIER JAVIER HENAO DÍXZ
Ing. SANDRA PATRICIA JUNCO ROMERO

Proyecto de Grado para optar al Título de Especialista en Seguridad Informática

Asesor: ÁLVARO ESCOBAR ESCOBAR
Ing. de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2017

Nota de aceptación

_____
_____
_____

_____
Firma presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C., septiembre de 2017

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

A la Universidad Piloto de Colombia, a todos los docentes de la especialización en seguridad Informática y en especial al Ing. Álvaro Escobar Escobar, asesor del proyecto de grado.

A la Corporación hospitalaria Juan Ciudad – MÉDERI, lideres, jefes y coordinadores de los diferentes procesos, en especial a la Ing. Constanza Rodríguez, jefe de TIC.

A todas aquellas personas que de una u otra forma colaboraron en la elaboración de este proyecto.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE GRÁFICAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACEPTACIÓN DEL RIESGO: decisión de asumir un riesgo.[1]

ACTIVO: cualquier cosa que tiene valor para la Organización.[2]

- Activos físicos: (hardware de computadores, servicios de comunicación, edificaciones)
- Información/datos (documentos, base de datos)
- Software
- Capacidad para suministrar un producto o servicio
- Personas Intangibles (imagen, reputación).

AMENAZA: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.[3]

ANÁLISIS DE RIESGO: uso sistemático de la información para identificar las fuentes y estimar el riesgo.[4]

AUTENTICIDAD: propiedad que garantiza que la identidad de un sujeto o recurso es la que se declara. La autenticidad se aplica a entidades tales como usuarios, procesos, sistemas e información.[5]

BCP (BUSINESS CONTINUITY PLAN): procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación debido a la interrupción. Nota: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio.[6]

---

[1] NORMA **TÉCNICA** COLOMBIANA. ISO 27000, Tecnología de la información - Técnicas de seguridad - Sistemas de administración de la seguridad de la información - Visión general y vocabulario. Colombia: ICONTEC, 2008,

[2]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Tecnología de la Información. Técnicas de Seguridad, Gestión de la Seguridad de la Tecnología de la Información y las Comunicaciones NTC 5411-1. Colombia: Mincit, 2013.

[3]NORMA **TÉCNICA** COLOMBIANA. ISO 27000. Op. cit. p. 16

[4]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Op. cit. p. 5

[5]Ibíd. .

[6]NORMA TÉCNICA COLOMBIANA. ISO 22301: Sistema de gestión de continuidad del negocio. Guía Técnica Colombiana GTC 176 Colombia: ICONTEC, 2013, 41 p.

BIA (BUSINESS IMPACT ANALYSIS): análisis de Impacto al Negocio (BIA) Herramienta utilizada por la organización para determinar, de manera cuantitativa y cualitativa, los impactos y pérdidas asociados a la no continuidad del negocio. Como resultado de este análisis se obtiene la información acerca de las funciones y procesos críticos del negocio, al igual que el nivel mínimo de recursos requeridos para asegurar la continuidad del negocio. Estos hallazgos son el insumo para la definición de las estrategias de continuidad y la toma de decisiones para la implementación de un programa de continuidad del negocio.[7]

CONTINUIDAD DEL NEGOCIO: capacidad de una organización para prevenir, atender, recuperar y restaurar las funciones criticas del negocio ante un evento, de tal forma que continúen, sin importar las circunstancias.[8]

CONFIABILIDAD: propiedad de tener comportamiento y resultados previstos consistentes.[9]

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni se divulgue a individuos, entidades o procesos no autorizados.[10]

CONTROL: en el contexto de la seguridad de la TIC, el término "control" se puede considerar sinónimo de "salvaguarda".[11]

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.[12]

DRP (Disaster Recovery Planner): Plan claramente definido y documentado el cual permite recuperar las capacidades de tecnología y telecomunicaciones cuando se presenta una interrupción.[13]

Es la estrategia que se seguirá para restablecer los servicios de TI (Hardware y Software), después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, daño premeditado, ataque de cualquier tipo el cual atente contra la continuidad del negocio.[14]

---

[7]NORMA TÉCNICA COLOMBIANA. Op.cit. p.16.
[8] Ibíd.
[9]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Op. cit. p. 5
[10] Ibíd.
[11] Ibíd.
[12]Ibíd,
[13] NORMA TÉCNICA COLOMBIANA. Op. Cit. p.6
[14] PLAN DE RECUPERACIÓN DE DESASTRES. ¿Qué es un drp? Colombia: DRP, 2012 p.1

GESTIÓN DEL RIESGO: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.[15]

GESTION DE CONTINUIDAD DEL NEGOCIO (GNC): proceso holístico y sistemático de la organización por medio del cual se identifican impactos potenciales que pueden amenazar la continuidad del negocio y provee un marco de referencias para establecer y desarrollar estrategias pro-activas, construir respuestas eficaces y eficientes con la flexibilidad y la capacidad necesarias (stakeholders), garantizar la gobernabilidad, la reputación, la imagen y las actividades de creación de valor de una organización.[16]

IMPACTO: resultado de un incidente de seguridad de la información.[17]

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos.[18]

RECUPERACIÓN DE DESASTRES: proceso de regresar una función de negocios a un estado de operaciones ya sea a un nivel interno de continuidad mínimo o restableciendo las operaciones a gran escala.[19]

RTO (Recovery Time Objetive): máximo lapso de tiempo durante el cual cada proceso se puede suspender antes de generar un impacto mayor. Este será el tiempo en el cual el proceso debe restablecerse, con sus recursos mínimos asociados, en caso de presentarse un evento que afecte la continuidad del negocio.[20]

RPO (Recovery Point Objetive): máxima pérdida tolerable de información para cada uno de los procesos evaluados.[21]

RIESGO: es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.[22]

---

[15]**CENTRO NACIONAL DE PREVENCIÓN DE DESASTRES.** *ISO 31000: 2009.* México: CENAPRED, 2007

[16]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Op.cit.p. 6

[17] Ibíd. p. 6.

[18]Ibíd.,p.6.

[19]NORMA TÉCNICA COLOMBIANA. Op.cit. p. 6

[20] Ibíd., p. 7

[21]Ibíd, p. 7

[22] NORMA TÉCNICA COLOMBIANA. Op.cit. p. 7.

RIESGOS DE TECNOLOGÍA: están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.[23]

RESILIENCIA: es la capacidad de un sistema de soportar y recuperarse ante desastres y perturbaciones.[24]

SISTEMA: conjunto de elementos interrelacionados que interactúan.[25]

SISTEMA DE INFORMACIÓN: es un conjunto de datos que interactúan entre sí con un fin común. Ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.[26]

SITIO ALTERNO: es un ambiente de características similares al sitio principal donde se dará continuidad a las tareas consideradas de mayor importancia para el negocio. Este sitio debe estar equipado con los recursos mínimos necesarios (escritorios, sillas, salas, computadoras, hojas de papel, etc.) para que el personal designado a trabajar en el sitio alterno pueda darle continuidad a las labores operativas hasta el periodo de tiempo que dure el restablecimiento del sitio principal.[27]

TRAZABILIDAD (Accountability): propiedad que garantiza las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.[28]

TRATAMIENTO DEL RIESGO: proceso de selección e implementación de medidas para modificar el riesgo.[29]

VALORACIÓN DEL RIESGO: proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.[30]

---

[23]DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía de Administración de Riesgos Colombia: Función Pública. 2015, 243 p.

[24] SIGNIFICADOS. COM. ¿Qué es resiliencia? [En línea], disponible en Internet en: https://www.significados.com/resiliencia/

[25] UNIVERSIDAD SANTIAGO DE CALI. Gestión de calidad, términos y definiciones. [En línea], disponible en Internet en: http://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones

[26] SIGNIFICADOS.COM. ¿Qué es sistema de información? [En línea], disponible en Internet en: https://www.significados.com/sistema-de-informacion/

[27]CXO2CSO.com. Sitio alterno y centro de procesamiento. [En línea], disponible en Internet en: http://www.cxo2cso.com/2015/02/sitioalterno-y-centro-de-procesamiento.html

[28] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Op.cit.p.7.

[29] Ibíd. p. 8.

[30] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. ISO/IEC27002. Bogotá: ICONTEC, 2005

VULNERABILIDAD: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.[31]

[31]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Op. cit, p, 8

INTRODUCCIÓN

En el entorno empresarial se está expuesto a diversos riesgos que pueden ser naturales, daños tecnológicos, incendios y errores humanos, los cuales deben ser listados, evaluados por los directivos y líderes de los procesos quienes determinarán cómo pueden llegar a ser su afectación dentro de la organización y cuanto de ese riesgo va a ser asumido por la entidad. Este análisis les permite tomar decisiones frente a las acciones pertinentes a tomar en cada uno de los eventos que pudiesen suceder, generando una documentación la cual le permitirá a la entidad en sus diferentes áreas reaccionar de manera ordenada, oportuna y eficaz en dichas situaciones, garantizando la capacidad de las operaciones de los diferentes servicios.

Dentro de la documentación generada al realizar el análisis por la entidad, se forma un documento identificado como plan de recuperación de desastre, el cual es el objeto de este documento, es el de dar inicio a la realización del plan de recuperación de desastres para el sistema de información Servinte, aplicación core del Hospital Méderi y la sede en Barrios Unidos, este sistema administra toda la información clínica de los pacientes (historias médicas, procedimientos, órdenes médicas etc.), inventarios de medicamentos, facturación, cartera, caja, contabilidad, este documento se desarrolla como opción de grado de la especialización en seguridad informática.

1. DEFINICIÓN DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

El hospital Méderi y su sede en barrios unidos al ser categorizado con servicios de cuarto nivel es uno de los más grandes y complejos que hay en la capital del país; el no contar con soluciones alternativas ante un desastre, las cuales tengan la capacidad de soportar la operación de hospital Méderi y sede en Barrios unidos, puede llegar a ser catastrófico en todos los niveles (financiero, reputacional, logístico, etc.) pero la consecuencia que impactará en gran medida ante una inoperatividad en los servicios críticos del hospital, es al ser humano, al servicio social y médico que se presta, el cual debe ser prioritario.

1.2 FORMULACIÓN DEL PROBLEMA

¿De qué forma se puede planear la continuidad de los procesos operativos administrados por el sistema SERVINTE en el hospital Méderi y la sede en Barrios Unidos, en caso de desastre?

2. JUSTIFICACIÓN

De acuerdo a la necesidad que presentan las empresas, independientemente de su actividad económica hoy en día, se ha visto la necesidad de tener un plan de recuperación a desastres, los cuales pueden ser ocasionados por fenómenos naturales, factores humanos voluntarios o involuntarios así como por fallas tecnológicas, que afecten el funcionamiento normal del hospital Méderi y su sede en Barrios Unidos, es necesario implementar un plan de recuperación de desastres de TI, este plan genera una herramienta en la cual se estipulan paso a paso el proceso de recuperación de desastres de TI para el sistema de información Servinte, frente a un eventual incidente que impacte negativamente el normal desarrollo de las actividades.

El Hospital Méderi y su sede Barrios Unidos no es ajeno a estos sucesos inesperados y de acuerdo a la prestación de los servicios en salud, siendo un hospital de cuarto nivel; la afectación que se tienen, al no prestar sus servicios a la comunidad es de gran impacto, es uno de los hospitales más grandes de la ciudad de Bogotá, en el cual se presta los servicios de hospitalización, urgencias, cuidados intensivos, consulta externa de diferentes especialidades, se ha visto la necesidad de implementar un plan de recuperación de desastres en todas las áreas del hospital, pero este documento se enfoca en la aplicación core de la institución llamado Servinte y su apropiado funcionamiento en el ámbito tecnológico. Este sistema de información maneja la información clínica de los pacientes (historias médicas, procedimientos, órdenes médicas, entre otras), inventarios de medicamentos, facturación, cartera, caja, contabilidad. Realizando el análisis de la criticidad que se presenta al no tener este sistema de información disponible para el correcto funcionamiento de la institución se ve la necesidad de realizar un plan de recuperación de desastre (DRP).

3. OBJETIVOS GENERALES Y ESPECÍFICOS

3.1 OBJETIVO GENERAL

Planificar la guía de reanudación y continuidad de las actividades y procesos relacionados con la aplicación SERVINTE del hospital Méderi y la sede de Barrios Unidos.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar y analizar los posibles riesgos que se pueden presentar determinando sus amenazas y vulnerabilidades.

- Identificar y evaluar el impacto que tendrá el hospital Méderi y su sede en Barrios Unidos de acuerdo a la criticidad de los procesos relacionados con la aplicación SERVINTE, los responsables, el tiempo de recuperación objetivo, el tiempo máximo tolerable fuera de servicio.

- Diseñar estrategias de recuperación y continuidad, enfocados en cada uno de los elementos que intervienen en los procesos relacionados con SERVINTE (infraestructura, sistemas, redes, hardware, bases de datos, personal).

- Diseñar pruebas que permitan ver el grado de optimización del plan de recuperación de desastre ante cualquier eventualidad.

4. MARCO DE REFERENCIA

4.1 MARCO INSTITUCIONAL

El hospital Méderi y la sede en Barrios Unidos es una organización que nació a partir de la adquisición del antiguo hospital San Pedro Claver propiedad del estado hace 9 años por parte de tres grandes organizaciones como son Compensar, Orden Hospitalaria San Juan de Dios y la Universidad del Rosario. Durante estos años la entidad ha tenido cambios en el mejoramiento de la prestación del servicio a los pacientes, contando con una capacidad de ocupación de camas de 800, realizando cambios de reforzamiento estructural y remodelación en algunos de sus 9 pisos, se ha preocupado por implementar avances tecnológicos con la modernización de las salas de cuidados intensivos, siendo una de las más grandes del país, preocupándose por prestar una buena atención y el bienestar de sus pacientes.

Este hospital cuenta con un departamento de tecnología y sistemas de la información el cual es el encargado adquirir, mantener, administrar la infraestructura tecnológica, esta área se ha preocupado por ofrecer las herramientas tecnológicas necesarias para que los colaboradores desempeñen sus actividades, una de estas herramientas es el sistema de información Servinte, el cual es el software que permite el manejo de la información clínica de los pacientes, facturación, cartera, suministros, activos fijos y contabilidad, este sistema se implementó hace más de 9 años desde que pasó de ser propiedad estatal a ser privada.

Después de toda la transición, estabilización y el trabajo que se ha realizado en pro de la certificación para alcanzar estándares de calidad de la organización en sus procesos, se vio la necesidad de iniciar un plan de recuperación de la entidad con respecto a su sistema de información principal, Servinte, ya que su indisponibilidad de servicio puede llegar a tener un impacto altamente negativo en los procesos internos de la corporación los cuales se identificaran mediante el BIA, llegando a afectar la atención oportuna de los pacientes. Teniendo en cuenta que el hospital está categorizado como de cuarto nivel y la atención al público es de 7 días por 24 horas, donde se atiende en un día promedio por el servicio de urgencias de acuerdo a su clasificación de triage I, II, III, alrededor de 1.500 personas, en el servicio de hospitalización un promedio de 800 personas y por último en el servicio de consulta externa se atienden un promedio de 400 personas.

El área de tecnología tiene la responsabilidad de mitigar el impacto que pueda llegar a ocasionar un evento de indisponibilidad del sistema de información Servinte, reanudar, estabilizar y poner en marcha su operación en el menor tiempo posible, causando el menor traumatismo en los diferentes servicios de acuerdo a toda la información que se maneja dentro de este sistema de información. Teniendo en cuenta que un plan de recuperación de desastres es una necesidad que toda entidad debe implementar y tener la capacidad de afrontar los riesgos a los que se

está expuesta, como se demuestra en la estadística publicada en el Global Disaster Recovery Índex 2012 por Acronis, en la cual muestra los incidentes que se han reportado por algunas entidades, seis mil funcionarios de Tecnologías de la Información (TI) reportaron que los desastres naturales causaron sólo 4% de las interrupciones de servicio, mientras incidentes en las instalaciones de los servidores (problemas eléctricos, fuegos y explosiones) representaron el 38%. Sin embargo, errores humanos, actualizaciones problemáticas y los virus encabezaron la lista con el 52%.[32]

Donde permite ver un panorama general de los riesgos más frecuentes a los que una empresa está expuesta permitiendo aterrizar sus propios riesgos, analizarlos con las personas involucradas de cada uno de los proceso dando pautas para la toma de decisiones, hasta qué punto se asume el riesgo, que acciones se deben tomar, que planes se van a tomar para su mitigación, enfocado siempre a disminuir su impacto, dar una continuidad al negocio y a sus procesos sin mayor afectación beneficiando no solo a la sostenibilidad de la empresa si no en la atención oportuna de los pacientes en una rama tan indispensable como lo es la salud.

Al generar una guía de plan de recuperación a desastres le permitirá al Hospital Méderi y la sede, actuar con eficacia frente algún evento que se llegase a presentar, biensea; natural, humano o falla tecnológica que pueda ocasionar una indisponibilidad de la aplicación Servinte.

4.2 MARCO TEÓRICO

4.2.1 Aspectos generales DRP. Este trabajo está enfocado en realizar un DRP (plan de recuperación de desastres), el plan de recuperación de desastres y el plan de continuidad del negocio pueden verse como conceptos muy ligados y parecidos, lo cierto es que el plan de continuidad de negocio está enfocado a fallos de cualquier elemento del entorno, necesario para el funcionamiento de un sistema, dicho estudio se realiza al detalle y abarcando toda una gama de amenazas y vulnerabilidades de todo tipo, el plan de recuperación de desastres en cambio estará enfocado a la recuperación de la actividad en este caso, informática y tecnología (hardware, software, datos) ante posibles desastres naturales, ataques, falla masiva o fallas humanas.

A través de la historia se ha podido ver grandes acontecimientos tanto desastres naturales como humanos, con los cuales se ha identificado la necesidad de tener planes de contingencia y recuperación, es totalmente cierto que la información es el

[32] PROMO ACRONIS. Acronis. Retrieved 10 2015, from Acronis: [Enlínea]. Disponible en Internet en http://promo.acronis.com/rs/acronis/images/DR_Index_2012_ShortVersion_US_ EN_120130.pdf

mayor “tesoro” con el que cuenta cualquier compañía y existen muchas personas malintencionadas e interesadas en obtener, destruir o modificar dicha información a cualquier precio, por fines económicos, políticos, religiosos etc.

Como ejemplo más claro y tal vez uno de los más mencionados es el ataque sufrido por los Estados Unidos a las torres gemelas en New York, a manos de grupos terroristas y extremistas:

- Un reciente estudio de Gartner, ratificó que las empresas que pasan por una crisis de pérdida de información tienen un alto riesgo de desaparecer en un tiempo estimado de 2 años. Una estadística alarmante para empresas que aún no cuentan con un sistema sólido de restauración de información. Así mismo, se afirma que el 60% de las compañías guardan una copia de seguridad de su información dentro de sus instalaciones, esto significa un alto riesgo para ellas, porque se puede perder la información original y la de respaldo.

- Vale la pena citar que, en 1993, cuando las torres gemelas en New York sufrieron un ataque terrorista, el 23% de las empresas quebraron por no tener un plan preventivo y de respaldo de su información. Caso contrario a lo que pasó en 2001 con la caída del WorldTrade Center, donde las empresas ya contaban con equipos de almacenamiento y planes de contingencia para situaciones como la que se presentaron en ese momento.

- Así mismo, en 2013, en España se realizó un estudio en el cual participaron profesionales de diferentes sectores industriales. El informe revela que hasta el 26% de los profesionales aceptaron haber eliminado datos por error de su empresa, de estos solo el 56% acudió a TI de su compañía para recuperar su información y el 20% restante aseguró no saber qué hizo su empresa para recuperarla.[33]

Dentro de los desarrollos e investigaciones que se han hecho específicamente para el campo de acción que se trata en este proyecto, “área hospitalaria”, existen algunas enfocadas con BCP, las cuales se entenderán más en detalle a continuación y de esta manera saber cómo se puede obtener un mayor provecho a la investigación:

Existe una investigación muy enfocada a este trabajo, desarrollada por John Erik Ángel Torres y Heynner Velasco Galeano, realizada en el 2014 en la Universidad Católica de Bogotá, el título de dicha investigación es: “diseño y propuesta de implementación de un plan de continuidad del negocio aplicable a los hospitales en la ciudad de Bogotá”.

[33] VISIÓN SOFTWARE, Seguridad de la información: sabía que la más mínima pérdida de información dentro de su empresa puede tener consecuencias irremediables. (2016, agosto). [En línea]. Disponible en internet en: http://www.visionsoftware.com.co/sabia-que-la-mas-minima-perdida-de-informacion-dentro-de-su-empresa-puede-tener-consecuencias-irremediables/

Los autores quisieron desarrollar un BCP completo enfocado a algunos de los hospitales de Bogotá como son: Hospital Occidente de Kennedy, Corporación hospitalaria Juan Ciudad Méderi, Hospital de Suba. El campo de acción abarcado por los autores es bastante amplio, ellos quisieron generalizar los procesos críticos de cada uno de los hospitales, identificando riesgos, vulnerabilidades, probabilidad de ocurrencia, impacto, retroalimentando de esta manera el plan para cada uno de los hospitales y reducir el riesgo de cada una de dichas amenazas y vulnerabilidades.

La metodología que desarrollaron fue de tipo investigativo, donde realizaron un análisis descriptivo del BCP, también fuentes de información, dentro de la cual utilizaron investigaciones, encuestas, para obtener el diagnóstico del objeto de investigación.

En la actualidad la mayoría o mejor, la totalidad de las empresas usan la tecnología como medio para llevar el control de sus procesos, por lo tanto, cada uno de los datos y la información que se genera toma vital importancia, según Natalia Sánchez, bloguera del portal de Celingest, empresa española dedicada a la optimización de recursos tecnológicos empresariales:

Un plan de recuperación ante desastres (DRP) es un proceso documentado o conjunto de procedimientos para recuperar y proteger la infraestructura tecnológica de una empresa en caso de un desastre.

Se llama desastre a cualquier causa que afecte a esta infraestructura (datos, hardware o software) ya sea natural, intencional o involuntario, e impida la continuidad del negocio.

Dada la creciente dependencia de las empresas a la tecnología de la información para dirigir sus operaciones, un plan de recuperación de desastres cobra cada día más relevancia, y por lo tanto, es indispensable que toda empresa disponga de él. Según IBM de las empresas que han tenido una pérdida principal de registros automatizados, el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años y sólo el 6 % sobrevivirá a largo plazo".[34]

Un DRP hace parte de un plan general llamado BCP (Business Continuity Plan) el cual también contiene: plan de reanudación de negocios, plan de emergencia personal, continuidad de operaciones y plan de manejo de incidentes. Este trabajo está enfocado única y exclusivamente al plan de recuperación de desastres (DRP) el cual se ocupa principalmente de la recuperación de procesos netamente

[34] SÁNCHEZ, Natalia. Plan de recuperación de desastres DRP (2013, marzo) disponible en DISASTER-RECOVERY. Recuperación desastres.http://blog.celingest.com/2013/03/01/ recuperación-desastres-disaster-recovery/

tecnológicos y no de los comerciales.

4.2.2 Norma ISO 22301. Para la realización de un DRP se requiere de un plan o una estrategia, un conjunto de pasos el cual se deberá seguir ordenadamente para llegar al producto final, para el desarrollo de este proyecto se tomará como marco de referencia la metodología propuesta por la norma ISO 22301 (Sistema de gestión de la continuidad del negocio), esta norma puede ser considerado una actualización de la BS 25999-2, con esta norma se podían certificar las empresas hasta mayo de 2012, a partir de esta fecha y hasta Noviembre de 2012 la certificación se realizó con las dos normas, pero a partir de Noviembre de 2012 la certificación para empresas solo fue posible con la norma ISO 22301, y las empresas que estaban certificadas con norma BS 25999-2 se tendría que actualizar a la nueva norma ISO 22301.

Se puede observar las principales diferencias entre dichas normas. (Ver cuadro 1)

Cuadro 1. Datos básicos normas BS 2999-2 vs ISO 22301

	Organización para la estandarizacion 22301	British StandardsInstitution 25999-2
Nombre completo	ISO 22301:2012 Seguridad de la sociedad sistemas de gestión de la continuidad de la continuidad del negocio - Requisitos	BS:25999-2 gestión de la continuidad del negocio, parte 2 : especificación
Publicada por	International OrganizationForStandardization	British StandardsInstitution
Fecha de publicación	15 de mayo de 2012	20 de Noviembre de 2007
Cantidad de páginas	24	28
Reconocida oficialmente	aceptada internacionalmente por institutos de normas nacionales en 163 países	Solo en el Reino Unido pero implementada Mundialmente
Fuente: autores		

Mediante la referencia de la norma ISO 22301, se tendrán las herramientas para poder identificar, clasificar y ponderar los factores internos y externos que puedan ser objeto de afectación en las actividades de la organización, obligaciones contractuales, suministros, servicios, funciones, productos, terceros, daños en la reputación y responsabilidades etc. También se tendrán lineamientos para establecer y definir políticas, valores, objetivos estratégicos. Etc.

Para desarrollar e implementar un DRP es de vital importancia el compromiso y

apoyo de la alta gerencia en cada uno de los procesos que se deben llevar a cabo la norma ISO 22301 específica en su apartado 5.7 Gestión de responsabilidades, el tipo de liderazgo y compromiso que debe tener la alta dirección:

> Para ser efectivo, un programa de IRBC debe ser un proceso completamente integrado con las actividades de gestión de la organización, direccionadas desde la alta gerencia de la organización, aprobadas y promovidas por la alta dirección. Un número de profesionales en el IRBC, practicantes y "Staff" de otras disciplinas y departamentos pueden ser requeridos para soportar y gestionar el programa IRBC. La cantidad de recursos requeridos para soportar tal programa dependerá del tamaño y complejidad de la organización.[35]

Según esto el grupo de gestión de continuidad como los procesos definidos deben formar parte de la dirección estratégica, garantizando los recursos necesarios, es importante también una comunicación a toda la empresa sobre la importancia de la gestión de continuidad del negocio y el plan a implementar DRP, se deberá velar por el alcance de los resultados esperados, estableciendo una política de continuidad del negocio y estableciendo roles y responsabilidades.

La gestión de continuidad del negocio para el establecimiento de un plan de recuperación de desastres desde el punto de estudio de ISO 22301, tiene como objetivo:

- Prevención: Por medio del establecimiento de planes de mejora y estrategias de recuperación se deberá proteger los servicios de informática y telecomunicaciones frente a las diferentes amenazas definidas.

- Detección: Monitorear, documentar y analizar constantemente cada uno de los elementos definidos en el inventario de activos con el fin de identificar evaluar y gestionar los riesgos a los que se está expuesto y en qué medida puede afectar, de esta manera tener una reacción inmediata y definida ante el incidente.

- Respuesta: Tener tiempos definidos de respuesta para así minimizar los tiempos de afectación y una posibilidad de reacción inmediata ante el incidente, de esta manera optimizando también los tiempos de recuperación.

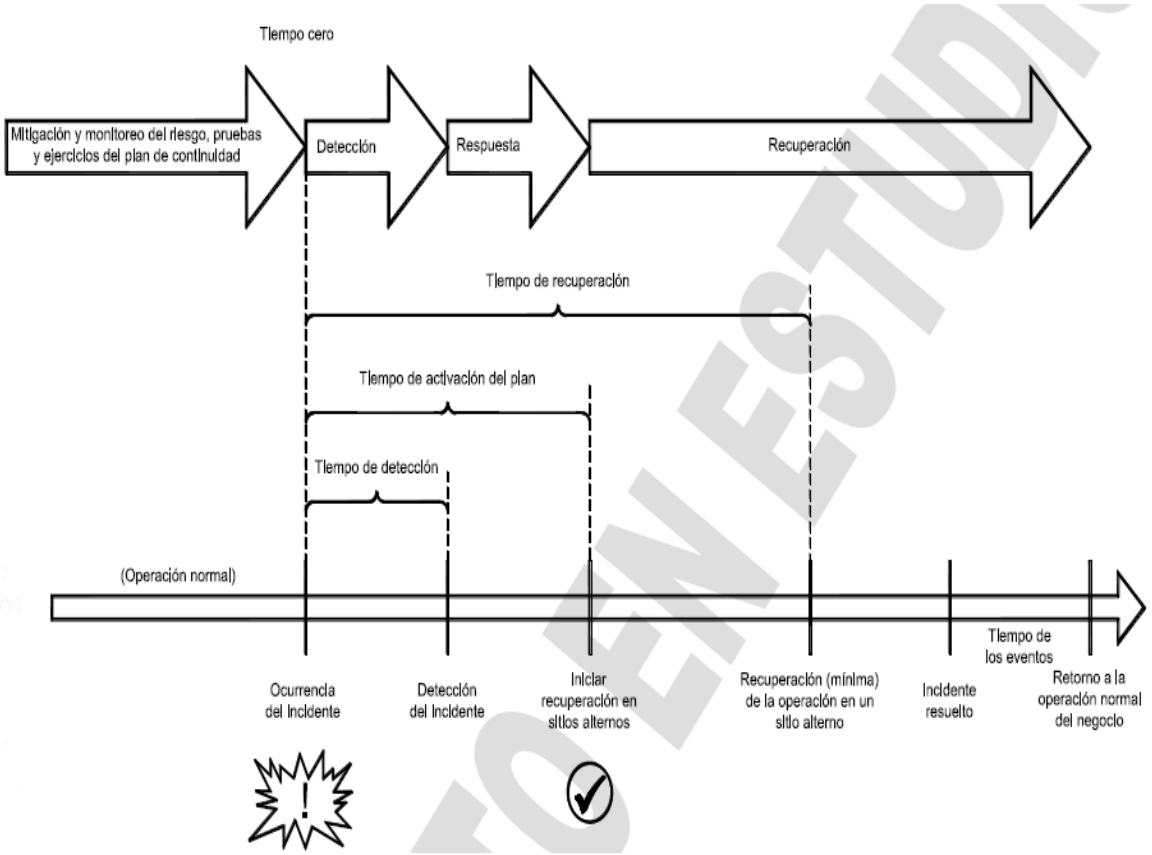
- Recuperación: En esta etapa se tendrá que garantizar primero que todo que los servicios y demás activos relacionados no dejaran de estar funcionales o bien no deberán sobrepasar los tiempos definidos para su recuperación, para esto se tendrán que definir muy bien las estrategias a utilizar que garanticen el restablecimiento del servicio sin afectar los pilares de la información; disponibilidad, confiabilidad e integridad.

[35] NORMA TÉCNICA COLOMBIANA. Op. cit. p. 11

- Mejoramiento: Para esta etapa se deberá recolectar toda la información que se generó anteriormente y retroalimentar el proceso mediante lecciones aprendidas, de esta manera lograr un mayor grado de preparación y madurez en el tratamiento de un incidente.

Se observa como la norma presenta el proceso de las etapas definidas anteriormente: (Ver figura 1)

Figura 1. Preparación de los elementos de tecnología y telecomunicaciones ICT para la continuidad del negocio



Fuente: NORMA TÉCNICA COLOMBIANA.Norma ISO 22301

ISO 22301 define 4 ciclos básicos para llevar a cabo el desarrollo del sistema de gestión de continuidad aplicados a la preparación de elementos de tecnología y comunicaciones (ICT): (Ver cuadro 2)

Para que una organización logre la preparación de las TIC para la Continuidad de Negocio (IRBC), es necesario poner en marcha un proceso sistemático destinado a prevenir, predecir y gestionar la interrupción o incidentes de las TIC que tengan la posibilidad de interrumpir los servicios de TIC. La mejor forma de alcanzarlo puede ser la utilización del ciclo PHVA (Planear, hacer, verificar y actuar), como parte de un sistema de gestión en TIC IRBC. De esta manera el IRBC apoya el BCM, asegurando que los servicios de las TIC son tan resistentes como adecuados y se pueden recuperar a niveles preestablecidos en los plazos requeridos y acordados por la organización.[36] (Ver figura 2)

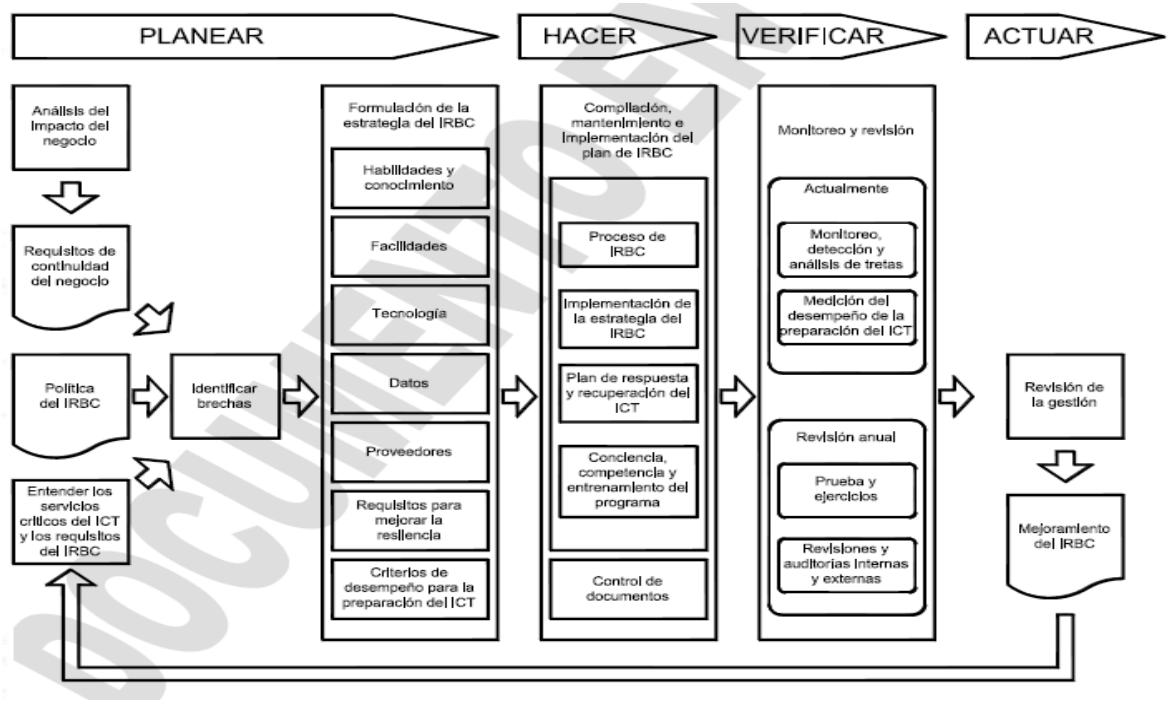
Cuadro 2. Definición del ciclo PHVA según norma ISO 22301

Planear	Establecer las políticas, objetivos, metas, procesos y procedimientos para el IRBC relacionados con el manejo de riesgos y el mejoramiento de la preparación de las TIC para el logro de resultados de acuerdo con unas políticas generales de continuidad del negocio para la Organización.
Hacer	Implementar y operar la política controles, procesos y procedimientos del IRBC.
Verificar	Evaluar y, cuando sea aplicable, medir el desempeño del proceso frente a las políticas, objetivos y experiencia del IRBC, y reportar los resultados a la dirección para su revisión.
Actuar	Tomar acciones correctivas y preventivas, basadas en la revisión de los resultados por la dirección, para alcanzar la mejora continua del IRBC.

Fuente: Norma ISO 22301

[36] NORMA TÉCNICA COLOMBIANA. Op. cit. p. 25

Figura 2. Etapas del IRBC



Fuente: Norma técnica colombiana ISO 22301

4.3 MARCO LEGAL

En el sector salud, el Ministerio de Salud y Protección Social es el ente regulador, que, por medio de leyes, resoluciones y decretos entre otras, estipulan la normatividad que las empresas prestadoras de salud deben implementar para prestar los servicios de salud a sus pacientes. El Hospital Méderi al usar el sistema de información Servinte da cumplimiento con la normatividad que regula la historia clínica y los registros clínicos.

La ley 23 del 1981 la cual reglamenta la norma de ética médica, en sus artículos 33 al 36 permiten que el médico cumpla con su ética profesional realizando los registros clínicos de acuerdo a sus conceptos médicos de forma clara, manteniendo la reserva y la disponibilidad que se requiera ante el paciente, terceros o en caso que la ley lo requiera.

La resolución 1995 de 1999 donde están establecidas las normas para el manejo de la historia clínica propende que toda entidad de salud tome las medidas necesarias para dar cumplimiento, brindando la integridad, secuencialidad, disponibilidad y seguridad, asegurando que la información clínica debe estar

disponible, al momento de ser consultada por el médico tratante con su paciente o porque el paciente así lo requiera. Al igual las instituciones deben contemplar los procesos de diligenciamiento, administración, custodia y confidencialidad de la historia clínica las cuales están consagradas en la ley 80 de 1989 del ministerio de salud y del archivo general de la nación.

Con la Ley 80 de 1980 el Congreso de la República de Colombia crean el archivo de la nación en la cual reglamentan la preservación, clasificación, organización y almacenamiento de los diferentes documentos ya sean históricos que sean de carácter público o privado, se administran con unas tablas de retención documental, en las cuales está estipulado el tiempo de almacenamiento, pasado este tiempo dependiendo del tipo de documento se puede proceder a los procesos de eliminación de dicha documentación para los registros clínicos el tiempo de conservación es de 20 años después de transcurrido este tiempo la entidad puede realizar los proceso de eliminación.

Algunas entidades hospitalarias y ambulatorias de manera voluntaria adoptan el proceso de ser una entidad acreditada en salud ambulatoria y hospitalaria, El Hospital Méderi por ser un hospital universitario debe acreditarse del mejoramiento continuo en la calidad en la prestación de servicios a sus pacientes este implementando este estándar desde hace tres años, este estándar está dividido en ocho estándares, los cuales abarcan los procesos de la entidad como son el Proceso de Atención al Cliente Asistencial, una segunda parte en la que se encuentran los proceso de Apoyo Administrativo-Gerencial. El proceso de tecnología de la información y telecomunicación al igual que todos los demás procesos se encuentra comprometido y ha estado apoyando en especial con los estándares de gestión de la tecnología y el estándar de la gerencia de la información los cuales aseguran que los elementos tecnológicos estén óptimos para el desarrollo de las actividades y la información esté disponible, íntegra y confiable, tanto al interior de la entidad y brindando la confianza a sus pacientes de la gestión que se realiza en el día a día en la institución.

En los últimos años ha aumentado la preocupación de la seguridad en los datos personales que manejan las entidades y por esto el gobierno expidió la Ley 1581 de 2012 protección de datos personales en la cual consagra la normatividad que se debe aplicar en todas las bases de datos donde se usen datos personales, asegurando que toda persona pueda conocer, actualizar y rectificar la información que repose en sus diferentes bases de datos ya sean físicas o lógicas. Las entidades de salud no son ajenas a esta ley ya que la información que usa y trata no solo es de identificación, ubicación, socioeconómico, si no que genera información de carácter sensible y son registrados en las historias clínicas por todo el personal asistencial que intervienen en la atención del paciente, el no cumplimiento de esta ley puede acarrear sanciones como cierre definitivo, temporal y multas económicas hasta los 2000 SMMLV.

4.4. ANÁLISIS DE LA SITUACIÓN ACTUAL.

Actualmente la infraestructura tecnológica del Hospital Méderi ha sufrido cambios considerables respecto a los estudiados en la anterior investigación, en la actualidad se cuenta con una granja de 36 servidores, los cuales están divididos en 32 de aplicaciones y 4 de componentes esta distribución permite que las dos sedes de la institución puedan tener acceso al sistema de información Servinte.

En una investigación desarrollada por el doctor Nelson Raúl Morales Soto[37], en Lima, Perú, establece una estrategia muy operativa en la cual concentra tres procesos prioritarios con los cuales pretende simplificar las acciones, y definir las responsabilidades de personas y equipos, de manera práctica y muy concisa, resumiéndose en cuadros de procesos, acciones y responsabilidades que se llevan a cabo por cada actor.

Para cada uno de los actores se crea una gama de riesgos más probables y sus probabilidades de manera muy directa, es decir que el Dr. Nelson Morales, quiso aplicar la preparación ante una amenaza al personal antes que lo técnico, complementando cada uno de los aspectos, es bastante interesante el enfoque que da el Dr. Nelson Morales, puesto que son las personas las que deberían estar muy bien preparadas psicológicamente y con destrezas agudas para enfrentar amenazas con el mayor profesionalismo y eficacia, si bien es cierto que se puede llegar a tener el mejor plan tecnológico para una recuperación de desastres, si no se tiene personal capacitado y listo para llevar a cabo cada una de las acciones planeadas, nada de lo realizado será óptimo.

> Es necesario identificar que un plan de recuperación de TI, proporciona unos procedimientos detallados a seguir, paso a paso, para recuperar los sistemas y redes que han sufrido disrupciones y ayudar a resumir la normalidad en las operaciones. El objetivo de estos procesos es minimizar cualquier impacto negativo en las operaciones de la compañía. El proceso de recuperación de desastres identifica los sistemas y redes críticos de TI; fija las prioridades para su recuperación y dibuja los pasos necesarios para reiniciar, reconfigurar y recuperar dichos sistemas y redes. Todo plan integral de recuperación de desastres debería incluir también a todos los proveedores relevantes, las fuentes de experiencia para recuperar los sistemas afectados y una secuencia lógica de los pasos a seguir hasta alcanzar una recuperación óptima.[38]

---

[37] MORALES SOTO, Nelson Raúl. Plan hospitalario para desastres. (2000). disponible en internet: http://www.planeamientohospitalario.info/contenido/referencia/PlanHospParaDesastres.pdf

[38] KIRVAN, P. Search Data Center. (2009, Octubre). (TechTarget) Retrieved 11 15, 2015 [en línea].Disponible en internet: http://searchdatacenter.techtarget.com/es/cronica/De-la-A-a-la-Z-plan-para-la-recuperación-de-desastres-RD-TI

Es realizar el análisis de las vulnerabilidades de las posibles indisponibilidades a las que está expuesta la organización con respecto al sistema de información Servinte, determinando su afectación a corto, mediano y largo plazo, identificando con qué recursos físicos, económicos y los actores con los que se cuenta para reaccionar en los eventos.

5. DISEÑO METODOLÓGICO

5.1TIPO DE INVESTIGACIÓN

El tipo de investigación en el que se basa este proyecto, es la investigación descriptiva, porqué se tendrá que ver en detalle cada uno de los riesgos o vulnerabilidades que puedan afectar la aplicación Servinte en el hospital Méderi y su sede en Barrios Unidos y como se puede prevenir y disminuir el impacto que se pueda generar dentro de la organización.

5.2 HIPÓTESIS

5.2.1 Hipótesis de investigación. El desarrollo del plan de recuperación y continuidad de las actividades y procesos relacionados con la aplicación SERVINTE en el hospital Méderi y la sede en Barrios Unidos, permitirá a la entidad tener un plan en situaciones de desastre o de indisponibilidad del servicio de la herramienta.

5.2.2 Hipótesis nula. El desarrollo de la guía de reanudación y continuidad de las actividades y procesos relacionados con la aplicación SERVINTE en el hospital Méderi y su sede, no le permitirá a la entidad tener un plan en situaciones de desastre o de indisponibilidad del servicio de la herramienta.

5.3 VARIABLES

5.3.1 Variable Independiente. Plan de recuperación de desastres

5.3.2 Variable Dependiente. Sistemas de información

5.3.3 Variable Interviniente. Hospital Méderi y su sede en Barrios Unidos, proceso de tecnología de la información y comunicación.

6. BIA SISTEMA DE INFORMACIÓN SERVINTE

Dentro del sistema de gestión de la seguridad de la información es necesario que Méderi cuente con un plan de recuperación de desastres en caso que suceda un evento que afecte la operación con respecto a la atención de los pacientes. Uno de los principales componentes que afecta en gran medida las operaciones que se presenta durante la atención de los pacientes es la no disponibilidad del sistema de información Servinte, el cual es una herramienta de apoyo, que permite llevar los registros clínicos y administrativos de los pacientes. Por la integridad que tiene esta aplicación es necesario contar con plan de recuperación del sistema, teniendo en cuenta todas las vulnerabilidades, amenazas a las que se están expuestos todos los componentes que permiten el funcionamiento de la aplicación y además identificar los procesos críticos a los cuales se les tendrá que dar prioridad a la hora de recuperar el servicio.

6.1 OBJETIVOS

Identificar los procesos críticos de negocio de Hospital Méderi y su sede en Barrios Unidos, administrados por medio de la aplicación Servinte, definiendo apropiadamente los RTO y RPO de cada uno de dichos servicios, según el nivel de impacto al momento de materializarse un desastre.

6.2 ALCANCE

Este plan de recuperación está definido cuando se presenta un contexto de no disponibilidad del sistema de información Servinte y del Datacenter, identificando las alternativas de restablecer en el menor tiempo las operaciones de los procesos que se afectaron, los cuales se encuentran definidos en la definición de procesos.

6.3 ENFOQUE UTILIZADO

Para el desarrollo del BIA se realizaron encuesta guiadas a los líderes de procesos con el objetivo de dar apoyo en la identificación de la criticidad de sus procesos, el tiempo de recuperación óptimo de los mismos y los diferentes tipos de impacto que podría llegar a tener la materialización de un incidente que afecte la disponibilidad del sistema de información Servinte.

Se realizaron las encuestas a los líderes de proceso de Hospital Méderi y su sede en Barrios Unidos definidos en el alcance, durante el mes de junio de 2017, dirigidas y apoyadas por la ingeniera Sandra Junco quien se desempeña como Oficial de seguridad informática de la entidad mencionada.

6.4 IDENTIFICACIÓN DE PROCESOS

El Hospital de Méderi está conformado por 46 procesos de los cuales 30 procesos usan Servinte para el desarrollo de sus actividades, teniendo en cuenta que todos no tiene la misma prioridad de recuperación al no tener disponibilidad del sistema, es necesario determinar su afectación, la prioridad y el tiempo de recuperación de los servicios. (Ver cuadro 3)

Cuadro 3. Procesos hospital Méderi

Nivel del proceso	Proceso
Gestión estratégica	Direccionamiento estratégico
	Planeación
Procesos misionales	Urgencias
	Clínicas medicas
	Clínicas quirúrgicas
	Salud sexual y reproductiva
	Cuidado critico
	Atención ambulatoria
	Programas especiales
	Atención cardiocirculatoria
	Investigaciones
	Educación médica
Procesos de apoyo asistencial	Nutrición
	Servicio farmacéutico
	Admisiones y autorizaciones
	Imágenes diagnosticas
	Patología
	Laboratorio clínico y servicio transfusional
	Referencia y contra referencia
	Rehabilitación
	Infecciones y vigilancia epidemiológica
	Enfermería
	Esterilización
	Paciente seguro

Cuadro 3. (Continuación)

Nivel del proceso	Proceso
Procesos de apoyo administrativo	Facturación
	Logística y suministros
	Gestión hotelera
	Jurídica
	Gestión ambiental
	Inteligencia de negocios
	Proyectos estratégicos y presupuesto
	Planta física
	Gestión contable
	Tecnología de la información y comunicaciones
	Mantenimiento
	Comercial y mercadeo
	Cartera
	Comunicaciones
	Archivo y documentos
	Tesorería
Procesos de apoyo transversal	Atención al usuario
	Talento humano
	Pastoral
	Gestión de la calidad
Procesos transversal	Gestión del riesgo
	Auditoría médica
Fuente: autores	

6.5 IDENTIFICACIÓN DE IMPACTO

Permite analizar el impacto que puede causar el no tener disponible un proceso por encontrarse ante un incidente o desastre. Los impactos contemplados y con los cuales se realizará la valoración serán los siguientes:

- Tiempo de afectación del proceso: Se debe evaluar el impacto que ocasionara no tener en operación el sistema Servinte de acuerdo a la cantidad de tiempo que dure dicha indisponibilidad.

- Reputación: Incluye la pérdida de confianza por parte de pacientes, clientes, proveedores, entidades de control, gubernamentales u opinión pública, a causa de un determinado evento que ocasione indisponibilidad del sistema Servinte el cual sea tratado de una manera no convencional.

- Financiero: se debe evaluar, durante la inoperatividad del sistema Servinte la no percepción de ingresos económicos, multas por incumplimiento de contratos y servicios.

- Servicio al Paciente: impacto que causa la indisponibilidad del programa Servinte en cuanto a la cantidad de tiempo que se puede ver afecta la adecuada prestación de cada uno de los servicios que se ofrecen en el Hospital Méderi y su sede en Barrios Unidos.

Para responder las preguntas los líderes de proceso deberán tener en cuenta los siguientes criterios. (Ver cuadro 4)

Cuadro 4. Criterios para definición de impacto

Valor	Impacto	Afectación del proceso	Reputación	Financiero	Servicio al paciente	Recurso humano
1	Bajo	Falla de la operación por 1 hora	al interior del proceso	Facturar < 1401 millones	tiempo máximo de recuperación sin causar afectación significativa es de 64 a 240 horas	No Requiere atención obligatoria de personal
2	Medio	Falla de operación por 6 Horas	conocimiento de número limitado de clientes	Facturar < 8409 millones	tiempo máximo de recuperación sin causar afectación significativa es de 48 a 64 horas	Requiere atención obligatoria por mínimo 1 persona
3	Alto	Falla de operación por 12 - 24 horas	Conocimiento de numero moderado de clientes	Facturar 16819 a 33638 millones	tiempo máximo de recuperación sin causar afectación significativa es de 24 a 48 horas	Requiere atención obligatoria por mínimo 5 persona
4	Extremo	Falla de operación por más de 24 horas	Conocimiento de medios de comunicación	Facturar > 33638 millones	tiempo máximo de recuperación sin causar afectación significativa es de 0 a 24 horas	Requiere atención obligatoria por mínimo >6 personas
Fuente: autores						

Cada uno del ítem mencionado anteriormente tendrá una ponderación porcentual de acuerdo a la valoración de impacto indicada por la dirección del Hospital Méderi; (Ver cuadro 5)

Cuadro 5. Ponderación porcentual de impacto

	Afectación del proceso	Reputación	Financiero	Servicio al paciente	Recurso humano
Porcentaje	0,15	0,15	0,25	0,35	0,10
Fuente: autores					

A continuación, se define las preguntas que se realiza a los líderes de cada uno de los procesos para definir el impacto de cada uno de los procesos en el hospital Méderi y su sede en Barrios Unidos, se observa el formato de cuestionario que será aplicado a los líderes de proceso. (Ver cuadro 6)

- Afectación del proceso

  - Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso en caso que se tenga indisponibilidad del sistema Servinte

- Reputación

  - Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso a nivel reputaciones teniendo en cuenta la opinión del cliente, proveedores, sector financiero, gubernamental y público en general.

- Financiero

  - Teniendo en cuenta la tabla de Criterios para definición de impacto, evalué cuánto dinero dejaría de percibir el hospital en caso de indisponibilidad del sistema Servinte

- Atención al paciente

  - Evalué el tiempo máximo que puede tardar la recuperación del sistema Servinte para no causar traumatismo en la atención a los pacientes del hospital Méderi y su sede en Barrios Unidos

- Recurso Humano

○ Mencione para su proceso que cantidad de personal es necesario para la apropiada operación del sistema Servinte

Cuadro 6. Formato definición de Impacto

Identificación de impacto	
Afectación del proceso	
Pregunta	Nivel de impacto
Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso en caso que se tenga indisponibilidad del sistema Servinte	
Reputación	
Pregunta	Nivel de impacto
Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso a nivel reputaciones teniendo en cuenta la opinión del cliente, proveedores, sector financiero, gubernamental y público en general.	
Financiero	
Pregunta	Nivel de impacto
Teniendo en cuenta la tabla de Criterios para definición de impacto, evalué cuánto dinero dejaría de percibir el hospital en caso de indisponibilidad del sistema Servinte.	
Atención al paciente	
Pregunta	Nivel de impacto
Evalué el tiempo máximo que puede tardar la recuperación del sistema Servinte para no causar traumatismo en la atención a los pacientes del hospital Méderi y su sede en Barrios Unidos	
Fuente: autores	

6.6 IDENTIFICACIÓN DE PROCESOS CRÍTICOS

Para la identificación de procesos críticos del Hospital Méderi y su sede en barrios unidos, se tendrá como base la calificación de impacto definida mediante el cuadro 5; y de acuerdo a los niveles de clasificación definidos por la gerencia de la siguiente manera:

- Todos los procesos que se encuentren calificados en el estudio de impacto como EXTREMO y ALTO serán tratados como procesos críticos para la misión del Hospital Méderi y su sede en Barrios Unidos, debido a que no contar con los mismos, la función del negocio no puede realizarse.

- Todos los procesos que se encuentren calificados en el estudio de impacto como MEDIO serán tratados como procesos críticos, puesto que, aunque no revistan gran impacto son parte integral para la operación.

- Todos los procesos que se encuentren calificados en el estudio de impacto como BAJO serán excluidos del plan de recuperación de desastres, puesto que según dicha calificación y según la dirección del hospital Méderi, no representan un gran riesgo para seguir operando, a estos procesos se les tendrá que hacer una reevaluación cuatrimestralmente con el fin de tener control de aumento de impacto para el negocio en dichos procesos.

Se puede observar la totalidad de procesos y la valoración obtenida mediante las entrevistas a cada uno delos líderes de proceso. (Ver cuadro 7)

Cuadro 7. Valoración de impacto de proceso

Proceso critico identificado	Proceso	Proceso ponderado 15%	Reputación	Reputación ponderado 15%	Financiero	Financiero ponderado 25%	Paciente	Paciente ponderado 35%	Recurso humano	Recurso humano ponderado 5%	Total	Impacto total
Direccionamiento estratégico	0	0	0	0	0	0	0	0	0	0	0	No aplica
Planeación	0	0	0	0	0	0	0	0	0	0	0	No aplica
Urgencias	4	0,6	3	0,45	4	1	4	1,4	4	0,4	3,85	Extremo
Clínicas medicas	4	0,6	3	0,45	4	1	4	1,4	4	0,4	3,85	Extremo
Clínicas quirúrgicas	3	0,45	3	0,45		0		0		0	0,9	Bajo
Salud sexual y reproductiva	2	0,3	2	0,3	2	0,5	3	1,05	2	0,2	2,35	Medio
Cuidado critico	4	0,6	4	0,6	3	0,75	4	1,4	3	0,3	3,65	Extremo
Atención ambulatoria	2	0,3	2	0,3	2	0,5	1	0,35	3	0,3	1,75	Bajo
Programas especiales	3	0,45	2	0,3	2	0,5	2	0,7	3	0,3	2,25	Medio
Atención cardiocirculatoria	2	0,3	2	0,3	1	0,25	1	0,35	3	0,3	1,5	Bajo
Investigaciones	1	0,15	1	0,15	1	0,25	1	0,35	2	0,2	1,1	Bajo
Educación médica	0	0	0	0	0	0	0	0	0	0	0	No aplica
Nutrición	2	0,3	2	0,3	2	0,5	3	1,05	3	0,3	2,45	Medio
Servicio farmacéutico	4	0,6	3	0,45	4	1	4	1,4	3	0,3	3,75	Extremo
Admisiones y Autorizaciones	4	0,6	4	0,6	3	0,75	4	1,4	3	0,3	3,65	Extremo
Imágenes diagnosticas	3	0,45	3	0,45	3	0,75	3	1,05	2	0,2	2,9	Alto
Patología	2	0,3	1	0,15	1	0,25	2	1		0	1,7	Bajo
Laboratorio clínico y servicio transfusional	3	0,45	3	0,45	2	0,5	3	1,05	3	0,3	2,75	Alto
Referencia y contra referencia	2	0,3	3	0,45	2	0,5	3	1,05	2	0,2	2,5	Medio
Rehabilitación	2	0,3	1	0,15	2	0,5	2	0,7	1	0,1	1,75	Bajo
Infecciones y vigilancia epidemiológica	1	0,15	1	0,15	1	0,25	1	0,35	2	0,2	1,1	Bajo
Enfermería	4	0,6	3	0,45	3	0,75	4	1,4	4	0,4	3,6	Extremo
Esterilización	0	0	0	0	0	0	0	0	0	0	0	No aplica
Paciente seguro	0	0	0	0	0	0	0	0	0	0	0	No aplica
Facturación	3	0,45	1	0,15	2	0,5	2	0,7	3	0,3	2,1	Medio
Logística y suministros	3	0,45	1	0,15	1	0,25	2	0,7	3	0,3	1,85	Medio

Cuadro 7. (Continuación)

Proceso Critico identificado	Proceso	Proceso ponderado 15%	Reputación	Reputación ponderado 15%	Financiero	Financiero ponderado 25%	Paciente	Paciente ponderado 35%	Recurso humano	Recurso humano ponderado 5%	Total	Impacto total
Gestión hotelera	0	0	0	0	0	0	0	0	0	0	0	No aplica
Jurídica	0	0	0	0	0	0	0	0	0	0	0	No aplica
Gestión ambiental		0		0		0		0		0	0	No aplica
Inteligencia de negocios	2	0,3	3	0,45	4	1	1	0,35	2	0,2	2,3	Medio
Proyectos estratégicos y presupuesto	0	0	0	0	0	0	0	0	0	0	0	No aplica
Planta física	0	0	0	0	0	0	0	0	0	0	0	No aplica
Gestión contable	2	0,3	1	0,15	1	0,25	1	0,35	2	0,2	1,25	Bajo
Tecnología de la información y comunicaciones	4	0,6	4	0,6	3	0,75	4	1,4	4	0,4	3,75	Extremo
Mantenimiento	0	0	0	0	0	0	0	0	0	0	0	No aplica
Comercial y mercadeo	1	0,15	1	0,15	1	0,25	1	0,35	2	0,2	1,1	Bajo
Cartera	3	0,45	2	0,3	3	0,75	1	0,35	2	0,2	2,05	Medio
Comunicaciones	0	0	0	0	0	0	0	0	0	0	0	No aplica
Archivo y documentos	1	0,15	2	0,3	1	0,25	2	0,7	1	0,1	1,5	Bajo
Tesorería	2	0,3	2	0,3	3	0,75	1	0,35	2	0,2	1,9	Medio
Atención al usuario	3	0,45	3	0,45	2	0,5	2	0,7	3	0,3	2,4	Medio
Talento humano	0	0	0	0	0	0	0	0	0	0	0	No aplica
Pastoral		0		0		0		0		0	0	No aplica
Gestión de la calidad	0	0	0	0	0	0	0	0	0	0	0	No aplica
Gestión del riesgo	1	0,15	2	0,3	1	0,25	1	0,35	3	0,3	1,35	Bajo
Auditoría médica	3	0,45	3	0,45	2	0,5	1	0,35	3	0,3	2,05	Medio
Fuente: autores												

Se listan los procesos críticos obtenidos. (Ver cuadro 8)

Cuadro 8. Procesos críticos identificados

Tipo de proceso	Nivel proceso	Proceso	Servinte	Impacto
Misionales	*Procesos misionales*	Urgencias	Si	Extremo
		Clínicas medicas	Si	Extremo
		Salud sexual y reproductiva	Si	Medio
		Cuidado critico	Si	Extremo
		Programas especiales	Si	Medio
Apoyo	*Procesos de apoyo asistencial*	Nutrición	Si	Medio
		Servicio farmacéutico	Si	Extremo
		Admisiones y autorizaciones	Si	Extremo
		Imágenes diagnosticas	Si	Alto
		Laboratorio clínico y servicio transfusional	Si	Alto
		Referencia y contra referencia	Si	Medio
		Enfermería	Si	Extremo
	Procesos de apoyo administrativos	Facturación	Si	Medio
		Logística y suministros	Si	Medio
		Inteligencia de negocios	Si	Medio
		Tecnología de la información y comunicaciones	Si	Extremo
		Cartera	Si	Medio
		Tesorería	Si	Medio
		Atención al usuario	Si	Medio
Evaluación	*Procesos de evaluación*	Auditoría médica	Si	Medio
Fuente: autores				

6.7 IDENTIFICACIÓN DE RTO

Para realizar la identificación del tiempo objetivo de recuperación se realiza la siguiente pregunta, con el fin de establecer el tiempo mínimo en el cual es necesario restablecer el servicio para dicho proceso sin que se cause una afectación a la

entidad.

Para que los líderes de proceso puedan determinar objetivamente la criticidad de su proceso se deberá guiar de acuerdo a los criterios de RTO. Además, se debe justificar adecuadamente la razón de su calificación. (Ver cuadro 9)

Cuadro 9. Criterios para definición de RTO

Nivel tiempo objetivo de recuperación	Tiempo objetivo de recuperación	Intervalo de recuperación
1	Critico	0 a 1 horas
2	Critico	1 a 8 horas
3	Alto	8 a 16 horas
4	Moderado	16 a 48 horas
5	Moderado	48 a 64 horas
6	Bajo	64 a 120 horas
7	Bajo	120 a 240 horas
Fuente: autores		

Se define la pregunta que se realiza a los líderes de procesos para determinar el RTO:

- Considere que ocurre un incidente de gran impacto que deja inoperante su proceso, de acuerdo a los criterios para definición de RTO; especifique el tiempo máximo que podría pasar cada uno de sus procesos antes de afectar considerablemente a la compañía (Tiempo Objetivo de Recuperación - RTO). (Ver cuadro 10)

Cuadro 10. Formato definición de RTO

Definición de tiempo objetivo de recuperación		
Pregunta	Tiempo objetivo de recuperación	Justificación
Considere que ocurre un incidente de gran impacto que deja inoperante su proceso, de acuerdo a los criterio para definición de RTO; especifique el tiempo máximo que podría pasar cada uno de sus procesos antes de afectar considerablemente a la compañía (Tiempo Objetivo de Recuperación - RTO).		
Fuente: autores		

Para ver un ejemplo de las entrevistas realizadas por favor remítase al anexo C. “Ejemplo de Cuestionario BIA para líderes de proceso, resuelto”

Después de aplicadas la encuesta descrita anteriormente se obtuvo los resultados relacionados (Ver cuadro 11)

Cuadro 11. Resultado RTO de procesos críticos

Tipo de proceso	Nivel proceso	Proceso	Tiempo objetivo de recuperación	Descripción	Justificación
Misionales	Procesos misionales	Urgencias	1	Proceso en el cual se brindan los servicios de urgencia a los pacientes que lo requieran.	Es el proceso por donde ingresan la mayoría de pacientes a la institución solicitando los servicios de salud con prioridad dependiendo de la clasificación de su estado de salud, realizando los registros en el módulo clínico es un servicio que debe estar en funcionamiento 7 x 24.
		Clínicas medicas	2	Proceso en el cual se presta los servicios de atención médica integral y especializada a los pacientes hospitalizados.	Es un servicio que realiza la atención con estancia de pacientes y es un servicio que ya bien con una atención anterior, este servicio tiene una disponibilidad de 7 x 24.
		Salud sexual y reproductiva	3	Servicio donde se da atención médica a las mujeres Gestantes y a los recién nacidos.	Se realizan registros clínicos de seguimiento de las madres gestantes y los recién nacidos, este servicio es una atención que funciona de lunes a sábado de manera ambulatoria, con una agenda médica.
		Cuidado critico	1	Servicio donde se presta a los pacientes cuidados de alta complejidad médica.	Se realizan registros clínicos de seguimiento y evolución de los pacientes críticos es un servicio que debe tener una disponibilidad de 7 x 24.

Cuadro 11. (Continuación)

Tipo de proceso	Nivel proceso	Proceso	Tiempo objetivo de recuperación	Descripción	Justificación
		Programas especiales	4	Servicio donde se le brinda al paciente una atención ambulatoria con patologías que requieren un control y seguimiento.	Se realizan registros clínicos de seguimiento y control de los pacientes de manera ambulatoria, con una agenda médica, de lunes a sábado.
Apoyo	Procesos de apoyo asistencial	Nutrición	5	Servicio donde se garantiza la atención nutricional integral, para el mejor desarrollo en la recuperación de los pacientes.	Es un servicio que de acuerdo a las recomendaciones clínicas realizadas en el sistema, el personal de nutrición formula las dietas especiales de cada paciente.
		Servicio farmacéutico	1	Servicio en el cual se dispensan los suministros (Medicamentos, insumos médicos) que son necesarios para el mejoramiento de la salud de los pacientes.	Es un servicio que necesita consultar las órdenes médicas generadas por los médicos de los diferentes servicios, para realizar la dispensación según criterio médico, este servicio debe tener una disponibilidad de 7 x 24.
		Admisiones y autorizaciones	1	Servicio en el cual se realiza el ingreso del paciente a la institución dando una priorización inicial, de acuerdo a su condición de salud, permitiendo la identificación del paciente y su prestador de servicios de salud. Asignación de Camas de acuerdo al servicio que sea indicado por el personal médico.	Servicio mediante el cual permite la identificación del paciente y su acompañante para el ingreso a la institución, asignándole un servicio y una ubicación, y de ser necesario los traslados de servicio según criterio médico. También realiza el proceso de autorización ante las EPS para la prestación de Servicios al paciente, es un servicio que su disponibilidad es de 7 x24.

Cuadro 11. (Continuación)

Tipo de proceso	Nivel proceso	Proceso	Tiempo objetivo de recuperación	Descripción	Justificación
Apoyo		Imágenes diagnosticas	1	Servicio donde se realizan gestionan las ordenes medicas relacionadas con imágenes diagnósticas, las cuales son enviadas a otro sistema de información con el cual realizan los procesos de Cita, procesado y permite la visualización de los exámenes realizados y a su vez enviando la lectura de los mismos por parte de los médicos especialistas en radiología a Servinte para así tener una trazabilidad de los exámenes realizados a los pacientes.	Este servicio atiende todos los requerimientos de ordenes medicas de imágenes diagnosticas de pacientes ambulatorios y hospitalarios para los servicios de Radiología Convencional, Radiología Especial, Radiología Intervencionista, Ecografía General, Tomografía, Ultrasonografía, Doppler, Mamografía, Resonancia y Medicina Nuclear, Este servicio es de una disponibilidad de 7x 24.
		Laboratorio clínico y servicio transfusional	1	Presta servicios de toma de muestras ambulatorias y procesamiento de muestras, en las áreas de Hematología, coagulación, química clínica, uro análisis, parasitología, microbiología, inmunología de acuerdo a las órdenes medicas generadas según criterio médico.	Este Proceso es prestado por un tercero el cual maneja sus sistemas de información, pero a su vez reporta los resultados de los análisis a Servinte por medio de una integración para los pacientes hospitalizados. En cuanto a los servicios de consulta externa son entregados directamente al paciente. Este servicio es necesario el funcionamiento 7 X 24

Cuadro 11. (Continuación)

Tipo de proceso	Nivel proceso	Proceso	Tiempo objetivo de recuperación	Descripción	Justificación
		Referencia y contra referencia	6	El proceso de referencia y contra referencia realiza las diferentes gestiones entre la sede de Barrios Unidos o con otras entidades con la debida autorización de la EPS ya sea un ingreso o un traslados, de acuerdo al estados de salud del paciente.	Este proceso realiza procesos administrativos como son los traslados o ingresos hacia la sede de Barrios Unidos, otras entidades prestadoras de servicios de salud.
		Enfermería	1	cuidado y seguimiento, a través de la ejecución de actividades independientes (cuidados básicos y específicos de enfermería), interdependientes (actividades compartidas con otras disciplinas) y dependientes (cumplimiento de órdenes médicas) que impacten en la recuperación, fortalecimiento del auto cuidado, satisfacción, mejoramiento del paciente	Este proceso intervienen durante toda la atención del paciente , brindando los cuidados necesario, realizando los registros clínicos de administración de medicamentos, líquidos, seguimiento del paciente entre otras, este servicio tiene un disponibilidad 7 x 24.
	Procesos de apoyo administra-tivos	Facturación	4	Proceso en el cual se facturan todos los registros de los cargos de los servicios prestados durante la atención del paciente y reportarlos a los prestadores que pertenece cada paciente.	Proceso en el cual se realiza el proceso de facturación de los cargos generados durante la atención de los pacientes, este proceso se realiza después que el paciente es dado de alta médica dando inicio al cobro de los servicios prestados a los prestadores.

Cuadro 11. (Continuación)

Tipo de proceso	Nivel proceso	Proceso	Tiempo objetivo de recuperación	Descripción	Justificación
		Logística y suministros	3	Proceso encargado de abastecer y mantener los insumos necesarios para la prestación de los servicios de los pacientes.	Este proceso basado en unos presupuestos del gasto mensual de los insumos realiza las órdenes de compra a los diferentes proveedores, asegurando la disponibilidad de acuerdo a la necesidad de cada uno de los servicios, este servicio realiza control, custodia y distribución a los diferentes servicios de los insumos.
		Inteligencia de negocios	4	Proceso el cual está encargado de generar la información unificada, oportuna de acuerdo a las necesidades empresariales, para la toma de decisiones de los diferentes servicios a si como Directivas.	Para la generación de los informes toma la información de Servinte por medio de una conexión a la BD con la herramienta en la se construyen los informes de acuerdo a la necesidad de los servicios.
		Tecnología de la información y comunica-ciones	1	Proceso en el cual gestiona y mantiene la disponibilidad de las diferentes herramientas tecnológicas para el desarrollo de las actividades corporativas tanto asistenciales como administrativas. Asegurando la disponibilidad, integridad y la confidencialidad de la información institucional.	TIC realiza el proceso de administrar los recursos y componentes tecnológicos para el funcionamiento del sistema de información Servinte, manteniendo la disponibilidad en las dos sedes.

Cuadro 11. (Continuación)

Tipo de proceso	Nivel proceso	Proceso	Tiempo objetivo de recuperación	Descripción	Justificación
		Cartera	7	Proceso mediante el cual realizan la radicación de cuentas medicas generadas con los cargos de los servicios prestados a los pacientes a los pagadores.	Proceso en el cual realizan la radicación de cuentas y realiza el cobro efectivo de la cartera
		Tesorería	3	Proceso el cual se encarga de registrar oportunamente y segura las transacciones de entradas y salidas de efectivo y cubrir las obligaciones de la corporación adquiridas a corto, mediano y largo plazo, administrando y gestionando los recursos en caja y bancos.	El ingreso de los pagos que realizan por la prestación de servicios, cuotas moderadoras en los diferentes servicios donde ser realiza el recaudo.
		Atención al usuario	4	Proceso en el cual brinda una interacción con el paciente y los familiares con los diferentes servicios de la institución ofreciendo una mejor atención institucional.	Un de las actividades de este servicio es dar ingreso a los familiares de los pacientes que se encuentra en hospitalización o urgencia, la información de la ubicación de los pacientes la toma de Servinte mediante un webservice, llevando un control de acceso de familiares a la institución
Evaluación	Procesos de evaluación	Auditoría médica	5	Proceso el cual evalúa, monitorea la calidad de la prestación de los servicios médicos, asegurando optimización de los recursos y calidad de los registro clínicos.	Para el desarrollo de las auditorias es necesario tener acceso a la información del proceso médico que se aplican a los pacientes, validando si son acertados o se debe realizara alguna mejora.

Fuente: autores

Se puede observar que se calificaron 12 procedimientos con un RTO crítico y alto a los cuales se tendrá que establecer una estrategia de recuperación prioritaria de 0 a 16 horas según lo establecido por la gerencia de hospital Méderi, los restantes 8 procedimientos fueron calificados con un RTO de entre 16 a 240 horas los cuales permiten un lapso de tiempo aun mayor para su recuperación. (Ver cuadro 12)

Cuadro 12. Análisis de RTO

Tipo de proceso	Intervalo	0 a 1 hora	1 A 8 horas	8 a 16 horas	16 a 48 horas	48 a 64 horas	64 a 120 horas	120 a 240 horas
	Nivel tiempo objetivo de recuperación	1	2	3	4	5	6	7
	Calificación	Critico	Critico	Alto	Moderado	Moderado	Bajo	Bajo
Misional	5	2	1	1	1	0	0	0
Apoyo	14	6	0	2	3	1	1	1
Evaluación	1	0	0	0	0	1	0	0
Estratégicos	0	0	0	0	0	0	0	0
Totales	20	8	1	3	4	2	1	1
	20	9		3	6		2	

Fuente: autores

6.8 IDENTIFICACIÓN DE RPO

El punto objetivo de recuperación, determina el máximo tiempo en el que el hospital Méderi y su sede en Barrios Unidos, está dispuesta a soportar la pérdida de operación por causa de indisponibilidad del sistema Servinte.

Para la identificación del RTO se realizan entrevistas a los líderes de cada uno de los procesos, mediante la cual se establece el tiempo máximo que cada proceso puede realizar sus operaciones manualmente, por causa de una falla tecnológica que ocasione inoperatividad del sistema Servinte, esto sin causar una afectación considerable a los servicios.

Mediante estas preguntas se establece de igual manera la periodicidad que se debería tener para las copias de respaldo, de acuerdo al nivel de riesgo que se defina por parte de la dirección. (Ver cuadro 13)

A continuación, se define las preguntas que se realiza a los líderes de cada uno de los procesos:

- ¿Existe para su proceso un procedimiento manual el cual se ejecuta en caso de falla del sistema Servinte?
- Diga cuánto tiempo puede trabajar su proceso de manera manual, sin que se vea afectado en gran medida el hospital Méderi y su sede en Barrios Unidos.

Cuadro 13. Formato definición de RPO

	Definición de punto objetivo de recuperación	
Numero	Pregunta	Respuesta
1.	¿Existe para su proceso un procedimiento manual el cual se ejecuta en caso de falla del sistema Servinte?	
2.	Diga cuánto tiempo puede trabajar su proceso de manera manual, sin que se vea afectado en gran medida el hospital Méderi y su sede en Barrios Unidos.	
Fuente: autores		

Para ver un ejemplo de las entrevistas realizadas por favor remítase al anexo C. "Ejemplo de Cuestionario BIA para líderes de proceso, resuelto"

6.8.1 Resultado RPO. Según la encuesta aplicada a los líderes de proceso anexo C "Ejemplo de Cuestionario BIA para líderes de proceso, resuelto", se muestra a continuación la tabla 4 de resumen de RPO necesarios para los procesos críticos definidos en el análisis de impacto: (Ver Cuadro 14)

Cuadro 14. Resumen de punto objetivo de recuperación en procesos críticos

Tipo de proceso	Nivel proceso	Proceso	Punto objetivo de recuperación
Misionales	*Procesos Misionales*	Urgencias	8 Horas
		Clínicas medicas	8 Horas
		Salud sexual y reproductiva	24 Horas
		Cuidado critico	8 Horas
		Programas especiales	24 Horas
Apoyo	*Proceso de apoyo asistencial*	Nutrición	96 Horas
		Servicio farmacéutico	8 Horas
		Admisiones y autorizaciones	8 Horas
		Imágenes diagnosticas	24 Horas
		Laboratorio clínico y servicio transfusional	24 Horas
		Referencia y contra referencia	48 Horas
		Enfermería	8 Horas
	Proceso de apoyo administrativo	Facturación	24 Horas
		Logística y suministros	48 Horas
		Inteligencia de negocios	96 Horas
		Tecnología de la información y comunicaciones	8 Horas
		Cartera	48 Horas
		Tesorería	48 Horas
		Atención al usuario	48 Horas
Evaluación	Proceso de evaluación	Auditoría médica	96 Horas
Fuente: Autores			

Teniendo en cuenta la clasificación de RPO se evidencia que el 35% de los procesos críticos puede tolerar máximo 8 horas de pérdida de información registrada mediante el sistema Servinte, 25% con un máximo tolerable de 24 horas, 25% con máximo tolerable de 48 horas y 15% con máximo tolerable de 96 horas, (Ver cuadro 15)

Con dicha información se establecerá un criterio de periodicidad de respaldo según el tiempo definido, en la estrategia de recuperación.

Cuadro 14. Resumen de resultados de punto objetivo de recuperación

Nivel	8 Horas	24 Horas	48 Horas	96 Horas
Crítico 1	6	2		
Crítico 2	1			
Alto 3		1	2	
Moderado 4		2	1	1
Moderado 5				2
Bajo 6			1	
Bajo 7			1	
Totales	7	5	5	3
	35 %	25 %	25 %	15 %
Fuente: autores				

6.9 IDENTIFICACIÓN DE INFRAESTRUCTURA Y RECURSO HUMANO TECNOLOGÍA)

Por medio de las siguientes preguntas realizadas al líder del proceso de Tecnología e infraestructura se pretende identificar:

Los módulos del sistema Servinte necesarios por cada uno de los procesos, el mínimo personal necesario para soportar la adecuada operación y funcionamiento dicho sistema y también los dispositivos de infraestructura necesarios para el adecuado funcionamiento del sistema Servinte.

Se observa el formato del cuestionario aplicado en la definición de la infraestructura y el recurso humano (Ver Cuadro 16)

- Mencione los módulos del sistema Servinte que utiliza cada uno de los procesos del hospital Méderi y su sede en Barrios Unidos los cuales garanticen su adecuada operación.

- Identifique que personal mínimo necesario para soportar la operatividad y funcionamiento de cada uno de los procesos del hospital Méderi y su sede de Barrio Unidos.

- Enumere cada uno de los elementos tecnológicos necesarios para el funcionamiento del sistema Servinte.

Cuadro 16. Formato definición de Infraestructura y recurso humano

Identificación de infraestructura y recurso humano				
Numero	Pregunta			
4.1	Mencione los módulos del sistema Servinte que utiliza cada uno de los procesos del hospital Méderi y su sede en Barrios Unidos los cuales garanticen su adecuada operación.			
4.2	Identifique que personal mínimo necesario para soportar la operatividad y funcionamiento de cada uno de los procesos del hospital Méderi y su sede de Barrio Unidos.			
4.3	Enumere cada uno de los elementos tecnológicos necesarios para el funcionamiento del sistema Servinte			
Proceso		4.1	4.2	4.3
Pregunta		Respuesta		
4.4	Relacione el personal que soporta e interviene en el apropiado funcionamiento del sistema Servinte			
Pregunta				
4.5	Relacione a continuación los elementos tecnológicos necesarios para el funcionamiento del sistema Servinte			
Tipo		Descripción	Cantidad sede mayor	Cantidad barrios unidos
Fuente: autores				

6.9.1 Resultados identificación recurso humano. Mediante la entrevista aplicada se obtuvieron los cargos relacionados, los cuales son necesarios para el apropiado funcionamiento, operación y soporte del sistema Servinte: (Ver Cuadro 17).

Cuadro 17. Identificación de recurso humano

Cargo	Cantidad
Jefe de tecnología y comunicaciones	1
Coordinador de infraestructura	1
Coordinador de base de datos	1
Coordinador de seguridad de la información	1
Administrados base de datos	1
Ingenieros de base de datos	4
Desarrollador	1
Ingeniero de imágenes diagnosticas	1
Jefe de enfermería de historia Clínica	1
Auxiliares de soporte clínico	4
Auxiliar data center	1
Técnicos de soporte	6
Fuente: Autores	

6.9.2 Resultado identificación elementos tecnológicos servinte. Mediante la entrevista aplicada se obtuvieron los elementos tecnológicos relacionados, necesarios para el apropiado funcionamiento, operación y soporte del sistema Servinte: (Ver Cuadro 18)

Cuadro 18. Identificación elementos tecnológicos Servinte

Ítem	Servinte	Sede mayor	Sede barrios unidos
Base de datos	Informix (Base de datos oracle) 6h	1	1(Replica)
Redes y comunicación	Routers	4	3
	swicth	40	16
	Firewall	2	1
	Canal de comunicaciones	etb y claro	une
	Internet	etb y claro	une
	Canal MPLS 16 servinte y 30 mbps imágenes	etb y claro	etb y claro
	Cableado estructurado	2500	500
Equipo auxiliar	Aire acondicionado	3	1
	UPS Smart UPS RT 6000 VA 50 kvas,30,29,10,6	8	3
	control de acceso	1	1
	detección y extinción de incendio	1	1
	control de temperatura y humedad	1	1
	Sistema cerrado de televisión	1	1
Fuente: Autores			

6.9.3 Resultado Identificación de software y módulos requeridos por proceso crítico. Mediante la entrevista aplicada, se obtuvo el siguiente software y módulos requeridos por los procesos críticos identificados, necesarios para el apropiado funcionamiento, operación y soporte del sistema Servinte. (Ver cuadro 19)

Cuadro 15. Identificación de software y módulos requeridos por proceso critico

Tipo de proceso	Nivel proceso	Proceso	Software	Infraestructura	Módulos	Estación de trabajo
Misionales	Procesos misionales	Urgencias	Servinte, Visor PDF, Agility, Mipres	Servidor de aplicaciones, servidor de componentes, Servidor de Impresión Internet, Servidor de PDF.	Tablero hospitalización(Historia Clínica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermería)	112
		Clínicas medicas	Servinte, Visor PDF, Agility, Mipres	Servidor de aplicaciones, servidor de componentes, servidor de impresión, servidor de PDF.	Tablero hospitalización(Historia clínica, evoluciones medicas, ordenes medicas, historia de enfermería)	208
		Salud sexual y reproductiva	Servinte, visor PDF, agility, mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión Internet, Servidor de PDF.	Tablero Clínico(Historia Clínica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermería)	10
		Cuidado critico	Servinte, visor PDF, agility, mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión	Tablero Clínico(Historia Clínica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermería)	55
				Internet, Servidor de PDF.		
		Programas especiales	Servinte, Visor PDF, Agility, Mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión	Tablero Clínico(Historia Clínica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermería)	15
				Internet, Servidor de PDF.		
		Nutrición	Servinte, Visor de PDF	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión	Tablero hospitalización(Historia Clínica, Evoluciones Medicas, ordenes medicas)	8

Cuadro 19. (Continuación)

Tipo de proceso	Nivel proceso	Proceso	Software	Infraestructura	Módulos	Estación de trabajo
				Internet, Servidor de PDF.		
		Servicio farmacéutico	Servinte, Visor de PDF	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión Manual, Servidor de Reportes.	Tablero hospitalización(ordenes medicas), Suministros	46
	Procesos de apoyo asistencial	Admisiones y autorizaciones	Servinte, Visor de PDF	Servidor de Aplicaciones, Servidor de Reportes, Servidor de Impresión Manual, Equipos de escritorio, Impresoras.	Tablero de Admisiones, Autorizaciones, Consulta de Tablero hospitalización.	11
		Imágenes diagnosticas	Servinte, Visor de PDF,Agility	Servidor de Aplicaciones, Servidor de Integraciones de Imágenes Diagnosticas	Tablero hospitalización(Historia Clínica, Evoluciones Medicas, Ordenes Medicas)	39
Apoyo		Laboratorio Clínico y Servicio Transfusional	Servinte, Visor de PDF	Servidor de Aplicaciones, Servidor de Integraciones Laboratorio	Tablero hospitalización (Historia Clínica, Ordenes Medicas), Facturación.	5
		Referencia y Contra referencia	Servinte, Visor de PDF	Servidor de Aplicaciones	Tablero hospitalización(ordenes Medicas)	5
		Enfermería	Servinte, Visor de PDF,Agility	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Integraciones Imágenes y Laboratorio, Servidor de PDF.	Tablero hospitalización(Historia Clínica, Ordenes Medicas, Historia de Enfermería)	30
	Procesos de apoyo administra-tivo	Facturación	Servinte, Visor de PDF.	Servidor de Aplicaciones, Servidor de Componentes, Servidor de impresión, Servidor de Reportes, Servidor de PDF.	Facturación(Análisis de Cuentas), Reportes	46
		Logística y suministros	Servinte, Docuclass	Servidor de Aplicaciones, Servidor de reportes, Servidor de impresión, impresora	Suministros, Cuentas por pagar, Maestros de suministros	15
		Inteligencia de negocios	Qlik View,Servinte	conexión a Base de datos	N/A	2
		Tecnología de la información y comunicaciones	Puty,Servinte, Visor De Pdf,Razor Sql, Agility	base de datos, Servidores de Aplicaciones, Servidores de componentes, Servidor de Reportes, Servidor de Impresión	Tablero Hospitalización, Tablero Consulta Externa, cartera, contabilidad, Cuentas por pagar, Facturación, caja y Bancos, Suministros, Reportes, Maestro del sistema	16

Cuadro 19. (Continuación)

Tipo de proceso	Nivel proceso	Proceso	Software	Infraestructura	Módulos	Estación de trabajo
		Cartera	Servinte, Visor de PDF	Servidores de Aplicaciones, Servidor de reportes, Impresora	Cartera	12
		Tesorería	Servinte, Visor de PDF	Servidor de Aplicaciones, Servidor de Reportes	Caja y Bancos	5
		Atención al usuario	Welcome, Almera	Conexión Base de datos	N/A	15
Evaluación	Procesos de evaluacion	Auditoría médica	Servinte, Visor de PDF, Mipres	Servidor de Aplicaciones, Servidor de reportes	Tablero de hospitalización(Historia Clínica, Historia de Enfermería, Ordenes medicas)	51
Fuente: Autores						

Se debe tener en cuenta que para el ítem infraestructura- Servidores, se utiliza un servidor por cada 25 usuarios de procesos clínicos y 30 usuarios en caso de procesos administrativos; y por cada 5 servidores de aplicaciones es necesario 1 servidor de componentes.

Se resume la cantidad de servidores necesarios para el funcionamiento de cada uno de los procesos críticos definidos en el análisis de impacto según la cantidad de usuarios por proceso: (Ver cuadro 20)

Cuadro 16. Cantidad de servidores necesarios por nivel de criticidad

Nivel	Usuarios	Servidor aplica-ciones	Servidor componentes	Servidor impresión	Servidor Pdf	Servidor integración de imágenes diagnosticas	Servidor integra-ción laboratorio	Servidor reporte	Servi-dor base de datos
Crítico 1	314	15	6	1*	1*	1*	1*	1*	1*
Crítico 2	208	8	2	1*	1*	0	0	0	1*
Alto 3	30	2	1	1*	1*	0	0	1*	1*
Mode-rado 4	78	5	2	1*	1*	0	0	1*	1*
Mode-rado 5	59	2	1	1*	0	0	0	1*	1*
Bajo 6	5	1	0	0	0	0	0	0	1*
Bajo 7	12	0	1	1*	0	0	0	1*	1*
Totales	706	33	13	1	1	1	1	1	1
Fuente: autores									

Se resaltan los procesos críticos que deberán tener prioridad de recuperación, los cuales, según la información obtenida, serán necesarios 25 servidores de aplicaciones, 9 servidores de componentes, 1 servidor de impresión, 1 servidor pdf, 1 servidor de integración de laboratorio, 1 servidor de integración de imágenes diagnósticas, 1 servidor de reportes, 1 servidor de base de datos, el servidor de backups será transversal a todos los procesos.

7. ANÁLISIS DE RIESGOS

7.1 DEFINICIÓN DEL ALCANCE

Para determinar qué estrategia que se puede implementar en el Hospital en el momento de tener una no disponibilidad de Servinte, se usó la metodología Magerit en su versión 3.0, esta metodología fue creada por el Concejo superior de Administración electrónica de España, está enfocada al análisis y gestión de los riesgos de los sistemas de información teniendo en cuenta para su valoración las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, permitiendo evaluar el impacto y el riesgo que puede tener si se materializan las amenazas sobre los activos que intervienen para el funcionamiento del sistema de información Servinte, aplicación Core de la institución y así plantear las posibles estrategias de recuperación que se pueden implementar.

Esta metodología consta de 9 actividades que son:

- Identificación de los activos
- Dependencia de los activos
- Valoración de los activos
- Identificación de las amenazas
- Valoración de las amenazas
- Identificación de los controles
- Valoración de los controles
- Estimación del Impacto
- Estimación del riesgo

7.2 IDENTIFICACIÓN DE LOS ACTIVOS

De acuerdo a la metodología de Magerit V3.0, permite identificar los diferentes activos de los que se componen los sistemas de información en una agrupación estándar como esta especificada a continuación. (Ver tabla 1)

Tabla 1. Tipos de Activos

Tipo de activo según Magerit v3.0
[INFO] Historias clínicas
[INFO ADM] Información administrativa
[SW] Aplicaciones / software
[HW] Equipos informáticos (hardware)
[COM] Redes de comunicaciones
[Media] Soportes de información
[AUX] Equipamiento auxiliar
[SS]Servicios subcontratados
[L] Instalaciones
[P] Personal
Fuente: Magerit - Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información Libro 1 – El Método

De acuerdo a la agrupación de activos se identifican los activos que interviene en el funcionamiento del sistema de información Servinte Core del hospital Méderi y su sede en Barrios Unidos. (Ver cuadro 21)

Cuadro 21. Activos del Sistema de Información Servinte

Activos Sistema De Información Servinte	
Activos Esenciales	
Informacion	Informacion Historias clínicas-administrativa
Aplicaciones / Software	
Software 1	Aplicación servinte clínica suite enterprise
Software 2	Sistemas operativos
Equipos informáticos (hardware)	
hardware 1	Servidores de aplicaciones
hardware 2	Servidores de componentes
hardware 3	Servidor de directorio activo
hardware 4	Servidor de integración laboratorio
hardware 5	Servidor de Integración Imágenes Diagnosticas
hardware 6	Servidor de Archivos PDF
hardware 7	Servidor de Impresión automática
Equipos informáticos (hardware)	
hardware 8	Servidor de impresión manual

Cuadro 21. (Continuación)

Activos Sistema De Información Servinte	
hardware 9	Servidor de reportes
hardware 10	Servidor de backup
hardware 11	Estaciones de trabajo
hardware 12	Servidor de base de datos Informix
Redes de comunicaciones	
comunicaciones 1	Switch, rourter
comunicaciones 2	Red local
Comunicaciones 3	Fw palo alto
Comunicaciones 4	Controladora de red
Equipamiento auxiliar	
Auxiliar 1	Sistema de alimentacion ininterumpida
Auxiliar 2	Aire acondicionado
Auxiliar 3	Controlador de temperatura y humedad
Auxiliar 4	Control de acceso
Servicios subcontratados	
Servicios subcontratados 1	Conexión a internet
Instalaciones	
Instalaciones 1	Centro de computo hospital mayor Méderi
Instalaciones 2	Centro de computo hospital barios unidos Méderi
Personal	
Personal 1	Usuarios funcionales
Personal 2	Jefe de tecnología y comunicaciones
Personal 3	Coordinador de Infraestructura
Personal 4	Coordinador de base de datos
Personal 5	Coordinador de seguridad de la información
Personal 6	Administrador de base de datos
Personal 7	Ingenieros de base de datos
Personal 8	Ingeniero de imágenes diagnosticas
Personal 9	Analista de data center
Personal 10	Técnicos de soporte
Personal 11	Jefe de enfermería de historia clínica
Personal 12	Auxiliares de soporte clínico
Fuente: autores	

Con la identificación de los activos, permite realizar la valoración del activo, identificando sus posibles amenazas y los posibles controles que permitan disminuir la probabilidad de ocurrencia.

7.3 DEPENDENCIA Y VALORACIÓN DE LOS ACTIVOS

Para la valoración de los activos, se tuvo en cuenta las siguientes dimensiones de seguridad como son:

Confidencialidad (C): La información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Integridad (I): Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Disponibilidad (D): Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.
Autenticidad (A): Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Trazabilidad (Acontability) (T): Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.[39]

La valoración numérica se realiza de acuerdo a las cinco dimensiones de valoración (D, I, C, A, T), si el activo tuviese alguna avería o daño que afectará el normal funcionamiento del sistema de información, se reflejará en la información que es el activo esencial, con esta valoración se evidencia cuan valioso es el activo frente a

[39] DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, Procedimientos e impulso de la Administración Electrónica, Metodología de Análisis y Gestión de Riesgos de los sistemas de información. Libro 1 – Método Pag.9. Madrid: Portal de Administración Electrónica.

cada una de las dimensiones de seguridad evidenciándose la criticidad de la no disponibilidad del activo. Teniendo en cuenta la valoración definida. (Ver Cuadro 22)

Cuadro 22. Valoración de los activos.

Criterios de valoración de los activos		
Valor	**Descripción**	**Criterio**
10	Nivel 10	daño extremadamente grave
9	Nivel 9	daño muy grave
8	Alto(+)	daño grave
7	Alto	daño grave
6	Alto (-)	daño grave
5	Medio (+)	daño importante
4	Medio	daño importante
3	Medio (-)	daño importante
2	Bajo (+)	daño menor
1	Bajo	daño menor
0	Bajo (-)	irrelevante a efectos prácticos
Fuente: Metodología de Análisis y Gestión De Riesgos de Los Sistemas de Información Libro 2 – Catálogo de Elementos p.19		

Con esta estimación de cada uno de los activos se identifica la dependencia entre cada uno de los activos, generándose una relación de funcionalidad entre activos principales con los activos segundarios, reflejándose la afectación o el daño de un activo como puede repercutir en el funcionamiento del sistema de información. (Ver cuadro 23)

Cuadro 23. Dependencia y valoración de los activos.

Activos		Dependencias	Valor	Criterios de valoración cuantitativa de los activos				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Activos Esenciales								
INFO	[INFO] Historias Clínicas-Administrativa	HW12,HW1,HW2,HW6,HW4,HW5,HW7,HW8,HW9,HW10,HW3,HW11,SW2,SW1	MA Muy Alta	10	10	10	10	10
SW1	Aplicación Servinte Clinical Suite Enterprise	HW12,HW1,HW2,HW6,HW4,HW5,HW7,HW8,HW9,HW10,HW3,HW11	MA Muy Alta	9	9	9	9	8
SW2	SO (Sistemas Operativos)	HW12,HW1,HW2,HW6,HW4,HW5,HW7,HW8,HW9,HW10,HW3,HW11	MA Muy Alta	9	8	7	7	9
[HW] Equipos informáticos (hardware)								
HW1	Servidores de Aplicaciones	AUX2,AUX1,AUX3,AUX4	MA Muy Alta	8	5	8	6	6
HW2	Servidores de Componentes	AUX2,AUX1,AUX3,AUX4	MA Muy Alta	8	5	8	6	
HW3	Servidor de directorio Activo	AUX2,AUX1,AUX3,AUX4	MA Muy Alta	9	5	7	6	
HW4	Servidor de Integración Laboratorio	AUX2,AUX1,AUX3,AUX4	M Media	7	7	5	4	
HW5	Servidor de Integración Imágenes DX	AUX2,AUX1,AUX3,AUX4	M Media	7	7	5	4	
HW6	Servidor de Archivos PDF	AUX2,AUX1,AUX3,AUX4	A Alta	7	9	9	9	8
HW7	Servidor de Impresión Automática	AUX2,AUX1,AUX3,AUX4	M Media	7				
HW8	Servidor de Impresión Manual	AUX2,AUX1,AUX3,AUX4	M Media	7				
HW9	Servidor de Reportes	AUX2,AUX1,AUX3,AUX4	M Media	5	3	8	2	6
HW10	Servidor de Backup	AUX2,AUX1,AUX3,AUX4	A Alta	10	10	10	8	8
HW11	Estaciones de trabajo	AUX2,AUX1,AUX3,AUX4	B Baja	6	5	5	5	5
HW12	Servidor de Base de datos Informix	AUX2,AUX1,AUX3,AUX4	MA Muy Alta	10	9	10	9	9
[COM] Redes de comunicaciones								
COM 1	Switch, Rourter	HW3,L1	A Alta	7	5	5	5	5
COM 2	Red Local	HW3,L1	MA Muy Alta	9	7	9	9	7
COM 3	Fw Palo Alto	HW3,L1	A Alta	9	9	9	9	7
COM 4	Controladora de Red	HW3,L1	MA Muy Alta	9	9	9	8	8

Cuadro 23. (Continuación)

Activos		Dependencias	Valor	Criterios de valoración cuantitativa de los activos				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
[AUX] Equipamiento auxiliar								
AUX1	UPS		MA Muy Alta	10				
AUX4	control de acceso	AUX1	A Alta	7				
[SS]Servicios Subcontratados								
SS1	Conexión a Internet	HW3,L1	M Media	8				6
[L] Instalaciones								
L1	Centro de Computo HUM	-	MA Muy Alta	10	10	8	8	9
L1	Centro de Computo HUBU	-	A Alta	9	8	8	8	8
[P] Personal								
P1	Usuarios Funcionales	No tiene dependencias	M Media	5				
P2	Jefe de Tecnología y Comunicaciones	No tiene dependencias	M Media	9				
P3	Coordinador de Infraestructura	No tiene dependencias	A Alta	9				
P4	Coordinador de Base de datos	No tiene dependencias	A Alta	9				
P5	Coordinador de Seguridad de la Información	No tiene dependencias	A Alta	8				
P6	DBA	No tiene dependencias	A Alta	9				
P7	Ingenieros de Base de datos	No tiene dependencias	A Alta	9				
P8	Ingeniero de Imágenes Diagnosticas	No tiene dependencias	M Media	7				
P9	Analista de data Center	No tiene dependencias	A Alta	9				
P10	Técnicos de soporte	No tiene dependencias	M Media	5				
P11	Jefe de enfermería de historia Clínica	No tiene dependencias	M Media	8				
P12	Auxiliares de soporte Clínico	No tiene dependencias	M Media	8				
Fuente: autores								

Con este ejercicio permite estimar el valor de cada uno de los activos y cómo puede afectar la materialización de las amenazas en las diferentes dimensiones. Se identifica sus dependencias, ya que cada uno de los activos depende de otro para realizar su finalidad, de esta manera un activo principal puede afectar su funcionamiento al presentar algún fallo de un activo secundario desencadenando una falla especifica o general que se refleja en el activo esencial que para nuestro caso es la información de historias clínicas y administrativas que es fuente para realizar el 90% de las actividades del hospital Mayor y su sede en Barrios Unidos.
Con esta valoración se identifica que los activos con mayor valor son los que contienen la información o su funcionalidad de comunicación entre los mismos, permitiendo que el sistema esté disponible, teniendo en cuenta que la prestación de servicios de salud debe tener una disponibilidad permanente de la información ya que para realizar los seguimientos o ingreso de la información de la atención del paciente al igual que el proceso administrativo con las diferentes EPS, proveedores entre otras debe estar en línea.

7.4 IDENTIFICACIÓN DE AMENAZAS, FRECUENCIAS E IMPACTO

Se realiza la identificación de las posibles amenazas que pueden afectar los activos teniendo en cuenta las amenazas del catálogo de Magerit V3.0, las cuales están clasificadas de origen Natural, origen industrial, defectos de aplicaciones, causadas por personal de forma accidental, causadas por personal de forma intencional, que pueden afectar algunos activos de maneras distintas. Con esta identificación permite identificar las vulnerabilidades que pueden llegarse a explotar por los diferentes tipos de amenazas y la frecuencia que se puedan presentar.

Para la estimación de frecuencias de ocurrencia se tomó la tabla de valoración de la metodología Magerit V3.0 con la cual se evalúa de cuerdo al conocimiento del personal, la posible ocurrencia de las amenazas, identificadas para cada uno de los activos. (Ver cuadro 24)

Cuadro 24. Probabilidad de Ocurrencia.

Probabilidad de ocurrencia		
Descripción	**Valor**	**Frecuencia**
MA Muy frecuente	100	Diario
A Frecuente	10	Mensualmente
M Normal	1	Una vez al año
B Poco frecuente	0,1	Cada varios años
MB Muy poco frecuente	0,01	Casi nunca
Fuente: Tabla probabilidad de ocurrencia - metodología de análisis y gestión de riesgos de los sistemas de información Libro 1 - Método Pag.28		

Para la estimación del impacto se tomó como base la probabilidad de ocurrencia de Magerit V3.0, manejando una mayor amplitud en la escala porcentual de afectación del impacto al ocurrir dicha amenaza sobre los activos. (Ver cuadro 25)

Cuadro 25. Impacto de la amenaza

Impacto degradación del valor de la amenaza	
Porcentaje	**Descripción**
100%	MA Muy alta
95%	MA Muy alta
90%	MA Muy alta
85%	A Alta
80%	A Alta
75%	A Alta
70%	M Media
60%	M Media
55%	M Media
50%	M Media
40%	B Baja
35%	B Baja
30%	B Baja
25%	B Baja
20%	MB Muy baja
15%	MB Muy baja
10%	MB Muy baja
5%	MB Muy baja
Fuente: autores	

Para la determinación de la probabilidad de ocurrencia de la amenaza sobre los diferentes activos se tomó como base la tabla de probabilidad de ocurrencia de la metodología Magerit V 3.0 modificando el tiempo en los cortes de semanal o menor, mensual, trimestral, semestral y anual o más para determinar su ocurrencia. Al igual para definir el impacto de la ocurrencia de la amenaza se valora en porcentaje determinando el impacto tiene sobre el activo dichas amenazas.

Se identifican por cada uno de los activos, las amenazas, frecuencias con la que

pueden ocurrir y el impacto que puede ocasionar si se llegase a explotar dicha amenaza sobre el activo. (Ver cuadro 26)

Cuadro 26. Amenazas, frecuencias e impacto sobre los activos.

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Activos Esenciales								
[INFO] Historias Clínicas-Administrativa								
[SW] Aplicaciones / Software								
Aplicación Servinte Clinical Suite Enterprise	[N] Desastres naturales	[I.5] Avería de origen físico o lógico	0,01	85%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	10	40%	80%	50%	80%	
		[E.4] Errores de configuración	1	90%	80%			
		[E.20] Vulnerabilidades de los programas (software)	1	90%				
		[E.21] Errores de mantenimiento / actualización de programas (software)	10	80%	50%	50%		
	[A] Ataques intencionados	[A.8] Difusión de software dañino	1	80%	50%	50%		
		[A.22] Manipulación de programas	0,1	80%	80%	80%		
		[A.11] Acceso no autorizado	0,1	50%	50%	70%		
SO (Sistemas Operativos)	[E] Errores y fallos no intencionados	[E.8] Difusión de software dañino	1	90%	20%	20%		
		[E.20] Vulnerabilidades de los programas (software)	10	80%	70%	50%		
		[E.21] Errores de mantenimiento / actualización de programas (software)	10	80%	80%			
	[A] Ataques intencionados	[A.8] Difusión de software dañino	1	75%				
		[A.22] Manipulación de programas	1	75%				
		[A.11] Acceso no autorizado	0,1	75%	60%			

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
[HW] Equipos informáticos (hardware)								
Servidores de Aplicaciones	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,1	100%				
		[I.6] Corte del suministro eléctrico	0,1	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	1	80%				
		[I.8] Fallo de servicios de comunicaciones	1	80%				
		[I.10] Degradación de los soportes de almacenamiento de la información	1	100%	80%			
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	1	75%	70%	75%		
		[E.2] Errores del administrador	1	75%	75%	75%		
		[E.8] Difusión de software dañino	10	80%	80%	80%		
		[E.18] Destrucción de información	0,01	90%				
		[E.19] Fugas de información	10			90%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[E.20] Vulnerabilidades de los programas (software)	1	80%	75%	75%		
		[E.21] Errores de mantenimiento / actualización de programas (software)	10	80%	75%	75%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	90%				
		[E.24] Caída del sistema por agotamiento de recursos	0,01	100%				
		[E.25] Pérdida de equipos	0,01	100%		20%		
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,01	80%	80%	50%		
		[A.5] Suplantación de la identidad del usuario	10		80%	90%	75%	
		[A.7] Uso no previsto	1		20%			
		[A.8] Difusión de software dañino	10	75%	75%	75%		
		[A.11] Acceso no autorizado	0,1	20%		70%	50%	
		[A.22] Manipulación de programas	0,1	90%	90%	90%		
		[A.23] Manipulación de los equipos	0,01	90%				
		[A.24] Denegación de servicio	1	90%				
		[A.25] Robo	0,01	50%		20%		
		[A.26] Ataque destructivo	0,01	90%	60%			
Servidor de Base de datos Informix	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,1	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%				
		[I.8] Fallo de servicios de comunicaciones	0,1	100%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,1	100%				
	[E] Errores y fallos no intencionados	[E.2] Errores del administrador	1	100%	75%	60%	35%	
		[E.8] Difusión de software dañino	0,01	100%	95%	90%	90%	
		[E.15] Alteración accidental de la información	1		90%	70%	80%	
		[E.19] Fugas de información	0,1			90%		
		[E.20] Vulnerabilidades de los programas (software)	0,1	90%	75%			
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	100%				
		[E.24] Caída del sistema por agotamiento de recursos	10	100%	75%			
		[E.25] Pérdida de equipos	0,01	100%				
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	1	100%	90%	80%		
		[A.5] Suplantación de la identidad del usuario	0,01		80%	90%	80%	
		[A.8] Difusión de software dañino	0,01	100%	80%	60%		
		[A.11] Acceso no autorizado	0,01	75%	75%	75%		
		[A.15] Modificación deliberada de la información	0,01		100%			

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.18] Destrucción de información	0,01	100%				
		[A.22] Manipulación de programas	0,01	75%	75%	75%		
		[A.23] Manipulación de los equipos	0,01	75%				
		[A.24] Denegación de servicio	0,01	100%				
		[A.25] Robo	0,01	100%		100%		
		[A.26] Ataque destructivo	0,01	100%				
Servidor de Reportes	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,1	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%				
		[I.8] Fallo de servicios de comunicaciones	0,1	100%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,1	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	0,1	20%	20%	20%		
		[E.2] Errores del administrador	1	20%	20%	20%		
		[E.8] Difusión de software dañino	0,01			5%		
		[E.18] Destrucción de información	0,01		5%			
		[E.19] Fugas de información	10			85%		
		[E.20] Vulnerabilidades de los programas (software)	1	75%	25%	75%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,01	75%				
		[E.24] Caída del sistema por agotamiento de recursos	0,01	100%				
		[E.25] Pérdida de equipos	0,01	100%				
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,01	80%	20%	50%		
		[A.5] Suplantación de la identidad del usuario	1		20%	75%	20%	
		[A.7] Uso no previsto	1		20%			
		[A.8] Difusión de software dañino	0,01	50%		50%		
		[A.11] Acceso no autorizado	1	50%		50%	50%	
		[A.15] Modificación deliberada de la información	0,01		20%			
		[A.18] Destrucción de información	0,01		20%			
		[A.22] Manipulación de programas	0,1	80%	30%			
		[A.23] Manipulación de los equipos	0,1	50%		50%		
		[A.24] Denegación de servicio	1	100%				
		[A.25] Robo	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
Servidor de Backup	[N] Desastres naturales	[N.1] Fuego	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.8] Fallo de servicios de comunicaciones	0,01	100%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,01	100%				
	[E] Errores y fallos no intencionados	[E.2] Errores del administrador	0,1	90%	85%	60%		
		[E.8] Difusión de software dañino	0,01	90%	75%	75%		
		[E.19] Fugas de información	0,01			75%		
		[E.20] Vulnerabilidades de los programas (software)	0,1	60%	80%	75%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	70%				
		[E.24] Caída del sistema por agotamiento de recursos	0,1	100%				
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,01	75%	75%	75%		
		[A.5] Suplantación de la identidad del usuario	0,1		80%	90%	60%	
		[A.7] Uso no previsto	1	75%				
		[A.8] Difusión de software dañino	1	85%				
		[A.11] Acceso no autorizado	0,1				60%	
		[A.15] Modificación deliberada de la información	1		80%			
		[A.18] Destrucción de información	1	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.22] Manipulación de programas	0,1	75%	75%	75%		
		[A.24] Denegación de servicio	0,1	75%				
Servidor de Impresión Automática	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	100%				
		[I.8] Fallo de servicios de comunicaciones	0,01	100%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,01	100%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	10	75%		50%		
		[E.2] Errores del administrador	1	50%	50%	50%		
		[E.8] Difusión de software dañino	0,1	50%	50%	50%		
		[E.20] Vulnerabilidades de los programas (software)	0,1	75%	50%	50%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	50%				
		[E.24] Caída del sistema por agotamiento de recursos	1	85%				
		[E.25] Pérdida de equipos	0,01	50%		20%		
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,01	50%	20%	20%		
		[A.5] Suplantación de la identidad del usuario	0,01		20%	20%	20%	
		[A.7] Uso no previsto	0,01		20%			
		[A.11] Acceso no autorizado	0,01	50%		20%		
		[A.22] Manipulación de programas	0,01	50%				
		[A.23] Manipulación de los equipos	0,01	50%				
		[A.24] Denegación de servicio	0,1	50%				
		[A.25] Robo	0,01	50%		20%		
Servidor de Impresión Manual	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	100%				
		[I.8] Fallo de servicios de comunicaciones	0,01	100%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,01	100%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	10	20%		5%		
		[E.2] Errores del administrador	1	50%	50%	50%		
		[E.8] Difusión de software dañino	0,01	50%	50%	50%		
		[E.20] Vulnerabilidades de los programas (software)	0,01		50%	50%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,01	20%				
		[E.24] Caída del sistema por agotamiento de recursos	1	50%				
		[E.25] Pérdida de equipos	0,01	50%		20%		
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,1	50%	20%	20%		
		[A.5] Suplantación de la identidad del usuario	0,01		20%	20%	20%	
		[A.7] Uso no previsto	0,1		20%			
		[A.8] Difusión de software dañino	0,01	50%	20%	20%		
		[A.11] Acceso no autorizado	0,01	50%		20%		
		[A.22] Manipulación de programas	0,1	50%	20%	20%		
		[A.23] Manipulación de los equipos	1	50%				
		[A.24] Denegación de servicio	0,1	50%		20%		
		[A.25] Robo	0,01	50%		20%		
		[A.26] Ataque destructivo	0,01	50%				
Servidor de Archivos PDF	[N] Desastres naturales	[N.1] Fuego	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	100%				
		[I.8] Fallo de servicios de comunicaciones	0,01	100%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,01	100%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	10	60%	80%	50%		
		[E.2] Errores del administrador	0,1	90%	75%	50%		
		[E.8] Difusión de software dañino	0,01	75%	90%	75%		
		[E.18] Destrucción de información	1	75%				
		[E.19] Fugas de información	0,1			95%		
		[E.20] Vulnerabilidades de los programas (software)	0,1	80%	50%	50%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	85%				
		[E.24] Caída del sistema por agotamiento de recursos	0,1	100%				
		[E.25] Pérdida de equipos	0,01	100%		90%		
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,1	75%				
		[A.5] Suplantación de la identidad del usuario	0,01		85%	85%	85%	
		[A.7] Uso no previsto	0,1		75%			
		[A.8] Difusión de software dañino	0,1	90%	75%	75%		
		[A.11] Acceso no autorizado	0,01	85%		90%	80%	
		[A.15] Modificación deliberada de la información	0,1		75%	75%		
		[A.18] Destrucción de información	0,1	90%				
		[A.22] Manipulación de programas	0,01	75%	75%	85%		
		[A.23] Manipulación de los equipos	0,01	60%		85%		
		[A.24] Denegación de servicio	0,01	95%				
		[A.25] Robo	0,01	100%		90%		
Servidores de Componentes	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	100%				
		[I.8] Fallo de servicios de comunicaciones	0,01	100%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,01	100%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	1	75%				
		[E.2] Errores del administrador	0,1	75%	75%			
		[E.8] Difusión de software dañino	0,1	85%				
		[E.21] Errores de mantenimiento / actualización de programas (software)	10	90%	70%			
		[E.20] Vulnerabilidades de los programas (software)	0,1	75%	75%	75%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	85%				
		[E.24] Caída del sistema por agotamiento de recursos	1	100%				
		[E.25] Pérdida de equipos	0,01	100%				
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,1	75%				
		[A.5] Suplantación de la identidad del usuario	0,1		75%	25%	35%	
		[A.7] Uso no previsto	0,1		75%			
		[A.8] Difusión de software dañino	0,1	80%	60%			
		[A.9] [Re-]encaminamiento de mensajes	0,01			90%		
		[A.11] Acceso no autorizado	0,01	85%	75%	70%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.22] Manipulación de programas	0,01	85%				
		[A.23] Manipulación de los equipos	0,01	90%				
		[A.24] Denegación de servicio	0,1	100%				
		[A.25] Robo	0,01	100%				
Servidor de Integración Laboratorio	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	90%				
		[I.8] Fallo de servicios de comunicaciones	0,01	85%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,01	100%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	0,1			50%		
		[E.2] Errores del administrador	1	50%	50%	50%		
		[E.8] Difusión de software dañino	0,01	50%	50%	50%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[E.9] Errores de [re-]encaminamiento	0,01			50%		
		[E.10] Errores de secuencia	10		50%			
		[E.19] Fugas de información	0,01			50%		
		[E.20] Vulnerabilidades de los programas (software)	0,1					
		[E.21] Errores de mantenimiento / actualización de programas (software)	10		50%	50%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,01	60%				
		[E.24] Caída del sistema por agotamiento de recursos	0,01	100%				
		[E.25] Pérdida de equipos	0,01	100%				
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,01	70%				
		[A.5] Suplantación de la identidad del usuario	0,01		60%		60%	
		[A.7] Uso no previsto	0,1		50%			
		[A.8] Difusión de software dañino	0,01	60%	50%	50%		
		[A.9] [Re-]encaminamiento de mensajes	0,01			50%		
		[A.11] Acceso no autorizado	0,1	70%		70%		
		[A.15] Modificación deliberada de la información	0,01		70%			
		[A.18] Destrucción de información	0,01	60%				
		[A.22] Manipulación de programas	0,01	60%	50%	50%		
		[A.23] Manipulación de los equipos	0,01	60%				
		[A.24] Denegación de servicio	0,01	100%				
		[A.25] Robo	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
Servidor de Integración Imágenes DX	[N] Desastres naturales	[N.1] Fuego	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(Contaminación 04 - Siniestro Mayor 06 - Fenómeno Climático 07 - Fenómeno Sísmico 08 - Fenómeno De Origen Volcánico 09 - Fenómeno Meteorológico 10 - Inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	90%				
		[I.8] Fallo de servicios de comunicaciones	0,01	85%				
		[I.10] Degradación de los soportes de almacenamiento de la información	0,01	100%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	0,1			50%		
		[E.2] Errores del administrador	1	50%	50%	50%		
		[E.8] Difusión de software dañino	0,01	50%	50%	50%		
		[E.9] Errores de [re-]encaminamiento	0,01			50%		
		[E.10] Errores de secuencia	10		50%			
		[E.19] Fugas de información	0,01			50%		
		[E.20] Vulnerabilidades de los programas (software)	0,1					

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[E.21] Errores de mantenimiento / actualización de programas (software)	10		50%	50%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,01	60%				
		[E.24] Caída del sistema por agotamiento de recursos	0,01	100%				
		[E.25] Pérdida de equipos	0,01	100%				
		[A.4] Manipulación de la configuración	0,01	70%				
		[A.5] Suplantación de la identidad del usuario	0,01		60%		60%	
		[A.7] Uso no previsto	0,1		50%			
		[A.8] Difusión de software dañino	0,01	60%	50%	50%		
		[A.9] [Re-]encaminamiento de mensajes	0,01			50%		
		[A.11] Acceso no autorizado	0,1	70%		70%		
		[A.15] Modificación deliberada de la información	0,01		70%			
		[A.18] Destrucción de información	0,01	60%				
		[A.22] Manipulación de programas	0,01	60%	50%	50%		
		[A.23] Manipulación de los equipos	0,01	60%				
		[A.24] Denegación de servicio	0,01	100%				
		[A.25] Robo	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
Servidor de directorio Activo	[I] De origen industrial	[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.8] Fallo de servicios de comunicaciones	0,01	100%				
	[E] Errores y fallos no intencionados	[E.2] Errores del administrador	1	90%	80%	75%		
		[E.8] Difusión de software dañino	0,1	75%	75%	75%		
		[E.19] Fugas de información	0,1			75%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[E.20] Vulnerabilidades de los programas (software)	0,1	90%	80%			
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	85%				
		[E.24] Caída del sistema por agotamiento de recursos	0,01	100%				
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	0,01	85%	75%			
		[A.5] Suplantación de la identidad del usuario	0,01		80%	80%	60%	
		[A.7] Uso no previsto	0,01	75%	75%	75%		
		[A.8] Difusión de software dañino	0,01	75%	75%	75%		
		[A.11] Acceso no autorizado	0,01		75%	75%		
		[A.15] Modificación deliberada de la información	0,01	75%	75%	75%		
		[A.18] Destrucción de información	0,01	100%				
		[A.22] Manipulación de programas	0,01	75%	85%			
		[A.24] Denegación de servicio	0,01	100%				
Estaciones de trabajo	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.*] Desastres naturales(Contaminación 04 - Siniestro Mayor 06 - Fenómeno Climático 07 - Fenómeno Sísmico 08 - Fenómeno De Origen Volcánico 09 - Fenómeno Meteorológico 10 - Inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	1	90%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[I.11] Emanaciones electromagnéticas	0,01	80%				
	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	10	50%				
		[E.4] Errores de configuración	1	75%				
		[E.8] Difusión de software dañino	10	60%	70%	50%		
		[E.18] Destrucción de información	10	50%				
		[E.20] Vulnerabilidades de los programas (software)	10	70%				
		[E.21] Errores de mantenimiento / actualización de programas (software)	10	75%				
		[E.25] Pérdida de equipos	10	100%				
	[A] Ataques intencionados	[A.4] Manipulación de la configuración	1		85%	85%		
		[A.5] Suplantación de la identidad del usuario	1		50%	50%	50%	
		[A.6] Abuso de privilegios de acceso	0,1		50%	50%		
		[A.7] Uso no previsto	1		50%	50%		
		[A.8] Difusión de software dañino	0,1	50%	50%	50%		
		[A.11] Acceso no autorizado	0,1		50%	50%		
		[A.22] Manipulación de programas	0,1		50%	50%		
		[A.24] Denegación de servicio	0,1	100%				
		[A.25] Robo	1	100%				
		[A.26] Ataque destructivo	0,01	100%				
[COM] Redes de comunicaciones								
Red Local	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	100%				
		[I.8] Fallo de servicios de comunicaciones	0,1	80%				
	[E] Errores y fallos no intencionados	[E.2] Errores del administrador	0,1	80%	75%	75%		
		[E.9] Errores de [re-]encaminamiento	0,1			75%		
		[E.10] Errores de secuencia	1		75%			
		[E.19] Fugas de información	0,1			75%		
		[E.20] Vulnerabilidades de los programas (software)	0,1	80%				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	85%				
		[E.24] Caída del sistema por agotamiento de recursos	0,1	100%				
		[E.25] Pérdida de equipos	0,01	75%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		75%			
		[A.18] Destrucción de información	0,01	75%				
		[A.23] Manipulación de los equipos	0,1	75%		50%		
		[A.24] Denegación de servicio	1	100%				
		[A.25] Robo	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
Fw Palo Alto	[N] Desastres naturales	[N.1] Fuego	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres naturales(Contaminación 04 - Siniestro Mayor 06 - Fenómeno Climático 07 - Fenómeno Sísmico 08 - Fenómeno De Origen Volcánico 09 - Fenómeno Meteorológico 10 - Inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				
		[I.7] Condiciones inadecuadas de temperatura o humedad	0,01	100%				
		[I.9] Interrupción de otros servicios y suministros esenciales	0,01	100%				
	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01	80%	85%			
		[E.18] Destrucción de información	0,01	75%				
		[E.19] Fugas de información	0,01			60%		
		[E.20] Vulnerabilidades de los programas (software)	0,1	95%	70%	90%		
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	70%				
		[E.24] Caída del sistema por agotamiento de recursos	0,01	100%				
		[E.25] Pérdida de equipos	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
	[A] Ataques intencionados	[A.5] Suplantación de la identidad del usuario	0,1		50%	50%	50%	
		[A.7] Uso no previsto	0,01	50%	50%	50%		
		[A.11] Acceso no autorizado	0,01	50%	50%	50%		
		[A.13] Repudio	0,01				50%	
		[A.15] Modificación deliberada de la información	0,01					
		[A.18] Destrucción de información	0,01		50%			
		[A.19] Divulgación de información	0,1			50%		
		[A.23] Manipulación de los equipos	0,1	50%		50%		
		[A.24] Denegación de servicio	0,1	85%				
		[A.25] Robo	0,01	100%		50%		
		[A.26] Ataque destructivo	0,1	50%				
Switch, Rourter	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
		[I.5] Avería de origen físico o lógico	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[I.8] Fallo de servicios de comunicaciones	0,01	100%				
	[E] Errores y fallos no intencionados	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	75%				
		[E.24] Caída del sistema por agotamiento de recursos	0,01	100%				
		[E.25] Pérdida de equipos	0,01	100%				
	[A] Ataques intencionados	[A.7] Uso no previsto	0,1	75%				
		[A.11] Acceso no autorizado	0,1		75%	75%		
		[A.15] Modificación deliberada de la información	0,01		75%			
		[A.23] Manipulación de los equipos	0,01	90%				
		[A.24] Denegación de servicio	0,01	95%				
		[A.25] Robo	0,01	100%				
		[A.26] Ataque destructivo	0,01	85%				
Controladora de Red	[I] De origen industrial	[I.8] Fallo de servicios de comunicaciones	0,01	100%				
	[E] Errores y fallos no intencionados	[E.2] Errores del administrador	1	85%	75%	75%		
		[E.9] Errores de [re-]encaminamiento	0,01			75%		
		[E.10] Errores de secuencia	0,1		75%			
		[E.19] Fugas de información	0,1			75%		
		[E.24] Caída del sistema por agotamiento de recursos	0,1	100%				
	[A] Ataques intencionados	[A.5] Suplantación de la identidad del usuario	0,1		75%	75%	75%	
		[A.7] Uso no previsto	0,1	75%	75%	75%		
		[A.9] [Re-]encaminamiento de mensajes	0,1			75%		
		[A.11] Acceso no autorizado	0,01		75%	75%	75%	
		[A.14] Interceptación de información (escucha)	0,01			90%		
		[A.15] Modificación deliberada de la información	0,01		85%	85%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.18] Destrucción de información	0,01	90%				
		[A.24] Denegación de servicio	0,01	100%				
[AUX] Equipamiento auxiliar								
UPS	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] Desastres Naturales(Contaminación 04 - Siniestro Mayor 06 - Fenómeno Climático 07 - Fenómeno Sísmico 08 - Fenómeno De Origen Volcánico 09 - Fenómeno Meteorológico 10 - Inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,1	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.9] Interrupción de otros servicios y suministros esenciales	1	100%				
Aire Acondicionado	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	1	100%				
		[I.*] Desastres industriales	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[I.3] Contaminación mecánica	0,01	100%				
		[I.6] Corte del suministro eléctrico	0,1	100%				
		[I.9] Interrupción de otros servicios y suministros esenciales	0,01	100%				
	[E] Errores y fallos no intencionados	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	100%				
	[A] Ataques intencionados	[A.7] Uso no previsto	0,01	60%				
		[A.23] Manipulación de los equipos	0,01	75%				
		[A.25] Robo	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
control de acceso	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
	[E] Errores y fallos no intencionados	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	90%				
	[A] Ataques intencionados	[A.7] Uso no previsto	0,01	50%				
		[A.23] Manipulación de los equipos	0,1	80%		50%		
		[A.25] Robo	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.26] Ataque destructivo	0,01	100%				
Controlador de Temperatura y Humedad	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[N.*] desastres naturales(contaminación 04 - siniestro mayor 06 - fenómeno climático 07 - fenómeno sísmico 08 - fenómeno de origen volcánico 09 - fenómeno meteorológico 10 - inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	50%				
	[E] Errores y fallos no intencionados	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,1	85%				
	[A] Ataques intencionados	[A.7] Uso no previsto	0,1	50%				
		[A.23] Manipulación de los equipos	0,01	80%				
		[A.25] Robo	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
[SS]Servicios Subcontratados								
Conexión a Internet	[I] De origen industrial	[I.8] Fallo de servicios de comunicaciones	1	90%				
	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		50%			
		[E.18] Destrucción de información	0,1	60%				
		[E.19] Fugas de información	0,01			80%		
	[A] Ataques intencionados	[A.5] Suplantación de la identidad del usuario	0,1		50%	60%	70%	
		[A.13] Repudio	0,1					60%

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.15] Modificación deliberada de la información	0,1			70%		
		[A.18] Destrucción de información	0,1	55%				
		[A.19] Divulgación de información	0,01	70%				
		[A.24] Denegación de servicio	0,1	100%				
[L] Instalaciones								
Centro de Computo HUM	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				
		[n.*] Desastres Naturales(Contaminación 04 - Siniestro Mayor 06 - Fenómeno Climático 07 - Fenómeno Sísmico 08 - Fenómeno De Origen Volcánico 09 - Fenómeno Meteorológico 10 - Inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
	[A] Ataques intencionados	[A.6] Abuso de privilegios de acceso	0,01	100%				
		[A.7] Uso no previsto	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
		[A.27] Ocupación enemiga	0,01	100%				
Centro de Computo HUBU	[N] Desastres naturales	[N.1] Fuego	0,01	100%				
		[N.2] Daños por agua	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[N.*] Desastres Naturales(Contaminación 04 - Siniestro Mayor 06 - Fenómeno Climático 07 - Fenómeno Sísmico 08 - Fenómeno De Origen Volcánico 09 - Fenómeno Meteorológico 10 - Inundación)	0,01	100%				
	[I] De origen industrial	[I.1] Fuego	0,01	100%				
		[I.2] Daños por agua	0,01	100%				
		[I.*] Desastres industriales	0,01	100%				
		[I.3] Contaminación mecánica	0,01	100%				
		[I.4] Contaminación electromagnética	0,01	100%				
	[A] Ataques intencionados	[A.6] Abuso de privilegios de acceso	0,01	100%				
		[A.7] Uso no previsto	0,01	100%				
		[A.26] Ataque destructivo	0,01	100%				
		[A.27] Ocupación enemiga	0,01	100%				
[P] Personal								
Usuarios Funcionales	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	100		75%			
		[E.19] Fugas de información	10			75%		
		[E.28] Indisponibilidad del personal	100	50%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	1		75%		75%	
		[A.18] Destrucción de información	0,01	100%	85%			
		[A.19] Divulgación de información	10			75%		
		[A.28] Indisponibilidad del personal	10	50%				
		[A.29] Extorsión	0,1	75%	75%	75%		
		[A.30] Ingeniería social (picaresca)	10	75%	75%	75%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Jefe de Tecnología y Comunicaciones	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		75%			
		[E.19] Fugas de información	0,01			75%		
		[E.28] Indisponibilidad del personal	10	50%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		75%		75%	
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01			75%		
		[A.28] Indisponibilidad del personal	1	50%				
		[A.29] Extorsión	0,01	75%	75%	75%		
		[A.30] Ingeniería social (picaresca)	0,01	75%	75%	75%		
Coordinador de Infraestructura	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		75%			
		[E.19] Fugas de información	0,01			75%		
		[E.28] Indisponibilidad del personal	10			75%		
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		50%			
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01	85%		75%		
		[A.28] Indisponibilidad del personal	1	75%				
		[A.29] Extorsión	0,01	75%	75%	75%		
		[A.30] Ingeniería social (picaresca)	0,01	75%	75%	75%		
Coordinador de Base de datos	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	10		90%			
		[E.19] Fugas de información	0,01			95%		
		[E.28] Indisponibilidad del personal	10	90%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		90%			

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01			95%		
		[A.28] Indisponibilidad del personal	0,1	90%				
		[A.29] Extorsión	0,01	90%	90%	90%		
		[A.30] Ingeniería social (picaresca)	0,01	95%	95%	95%		
Coordinador de Seguridad de la Información	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		40%			
		[E.19] Fugas de información	0,01			95%		
		[E.28] Indisponibilidad del personal	10	90%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		60%			
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01			95%		
		[A.28] Indisponibilidad del personal	0,1	90%				
		[A.29] Extorsión	0,01	90%	90%	90%		
		[A.30] Ingeniería social (picaresca)	0,01	95%	95%	95%		
DBA	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	10		90%			
		[E.19] Fugas de información	0,01			95%		
		[E.28] Indisponibilidad del personal	10	90%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		90%			
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01			95%		
		[A.28] Indisponibilidad del personal	0,1	90%				
		[A.29] Extorsión	0,01	90%	90%	90%		
		[A.30] Ingeniería social (picaresca)	0,01	95%	95%	95%		

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Ingenieros de Base de datos	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	10		90%			
		[E.19] Fugas de información	0,01			95%		
		[E.28] Indisponibilidad del personal	10	90%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		90%			
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01			95%		
		[A.28] Indisponibilidad del personal	0,1	90%				
		[A.29] Extorsión	0,01	90%	90%	90%		
		[A.30] Ingeniería social (picaresca)	0,01	95%	95%	95%		
Ingeniero de Imágenes Diagnosticas	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		90%			
		[E.19] Fugas de información	0,01			95%		
		[E.28] Indisponibilidad del personal	10	90%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		90%			
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01			95%		
		[A.28] Indisponibilidad del personal	0,1	90%				
		[A.29] Extorsión	0,01	90%	90%	90%		
		[A.30] Ingeniería social (picaresca)	0,01	95%	95%	95%		
Analista de data Center	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		75%			
		[E.19] Fugas de información	0,01			75%		
		[E.28] Indisponibilidad del personal	10			75%		
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		50%			
		[A.18] Destrucción de información	0,01	100%				

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[A.19] Divulgación de información	0,01	85%		75%		
		[A.28] Indisponibilidad del personal	0,1	75%				
		[A.29] Extorsión	0,01	75%	75%	75%		
		[A.30] Ingeniería social (picaresca)	0,01	75%	75%	75%		
Técnicos de soporte	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		20%			
		[E.19] Fugas de información	0,01			75%		
		[E.28] Indisponibilidad del personal	10	60%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01	70%				
		[A.18] Destrucción de información	0,01	100%				
		[A.19] Divulgación de información	0,01			75%		
		[A.28] Indisponibilidad del personal	0,1	60%				
		[A.29] Extorsión	0,01	75%	75%	75%		
		[A.30] Ingeniería social (picaresca)	0,01	75%	75%	75%		
Jefe de enfermería de historia Clínica	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		95%			
		[E.19] Fugas de información	0,01			90%		
		[E.28] Indisponibilidad del personal	10	90%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		75%			
		[A.18] Destrucción de información	0,01	85%				
		[A.19] Divulgación de información	0,01			95%		
		[A.28] Indisponibilidad del personal	0,1	95%				
		[A.29] Extorsión	0,01	75%	75%	75%		
		[A.30] Ingeniería social (picaresca)	0,01	75%	75%	75%		
Auxiliares de soporte Clínico	[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	0,01		95%			

Cuadro 26. (Continuación)

Activos sistema de información Servinte	Tipo de amenaza	Amenazas	Frecuencia cuantitativa	Impacto sobre dimensión del activo				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
		[E.19] Fugas de información	0,01			90%		
		[E.28] Indisponibilidad del personal	10	90%				
	[A] Ataques intencionados	[A.15] Modificación deliberada de la información	0,01		75%			
		[A.18] Destrucción de información	0,01	85%				
		[A.19] Divulgación de información	0,01			95%		
		[A.28] Indisponibilidad del personal	0,1	95%				
		[A.29] Extorsión	0,01	75%	75%	75%		
		[A.30] Ingeniería social (picaresca)	0,01	75%	75%	75%		

7.5 IDENTIFICACIÓN DE CONTROLES

Se realiza la identificación de controles que pueden disminuir la probabilidad de ocurrencia o el impacto sobre las diferentes amenazas de cada uno de los activos, esta identificación se realizó basada en el estándar NTC-ISO/IEC 27002:2013, Méderi y su sede en Barrios Unidos que es una entidad que está iniciando en la implementación del sistema de gestión de seguridad de la información SGSI, por este motivo se realizó una valoración de madurez, tomando como guía los estándares NTC-ISO/IEC 27000, ya que existían una gestión de documentación, implementación y control sobre los componentes tecnológicos que se manejan al interior de proceso de tecnología, al tomar este estándar internacional como referencia, permite optimizar la valoración, el control y plantear estrategias para mitigar los riesgos que se tiene sobre los componentes tecnológicos de la institución.

Se tomaron algunos controles que ayudaron a disminuir probabilidad de ocurrencia de las amenazas y a su vez mitigar el impacto que pueden ocasionar y así disminuir el riesgo de los activos. (Ver cuadro 27)

Cuadro 17. Identificación de controles para las amenazas de los activos Servinte

Tipo de amenaza	Amenaza	Control	
[A] Ataques intencionados	[A.11] Acceso no autorizado	9.1.1	Política de control de acceso
[A] Ataques intencionados	[A.13] Repudio	12.4.1	Registro de eventos
[A] Ataques intencionados	[A.14] Interceptación de información (escucha)	13.1	Gestión de la seguridad de las redes
[A] Ataques intencionados	[A.15] Modificación deliberada de la información	12.4.3	Registros del administrador y del operador
[A] Ataques intencionados	[A.18] Destrucción de información	12.3.1	Respaldo de la información
[A] Ataques intencionados	[A.19] Divulgación de información	7.2.2	Toma de conciencia, capacitación y formación en la seguridad de la información
[A] Ataques intencionados	[A.22] Manipulación de programas	9.4	Control de acceso a sistemas y aplicaciones
[A] Ataques intencionados	[A.23] Manipulación de los equipos	8.1.3	Uso aceptable de los activos
[A] Ataques intencionados	[A.24] Denegación de servicio	14.2	Seguridad en los procesos de desarrollo y de soporte
[A] Ataques intencionados	[A.25] Robo	9.1	Requisitos del negocio para control de acceso
[A] Ataques intencionados	[A.26] Ataque destructivo	9.2	Gestión de acceso de usuarios
[A] Ataques intencionados	[A.27] Ocupación enemiga	11.1.2	Controles de acceso físicos
[A] Ataques intencionados	[A.28] Indisponibilidad del personal	6.1.2	Segregación de deberes
[A] Ataques intencionados	[A.29] Extorsión	6.1.3	contacto con las autoridades
[A] Ataques intencionados	[A.30] Ingeniería social (picaresca)	7.2.2	Toma de conciencia, capacitación y formación en la seguridad de la información
[A] Ataques intencionados	[A.4] Manipulación de la configuración	9.2.5	Revisión de los derechos de acceso de usuarios
[A] Ataques intencionados	[A.5] Suplantación de la identidad del usuario	9.4.3	Sistema de gestión de contraseñas
[A] Ataques intencionados	[A.6] Abuso de privilegios de acceso	9.2.2	Suministro de acceso de usuarios
[A] Ataques intencionados	[A.7] Uso no previsto	13.1.2	Seguridad de los servicios de red
[A] Ataques intencionados	[A.8] Difusión de software dañino	12.2.1	Controles contra códigos maliciosos

Cuadro 27. (Continuación)

Tipo de amenaza	Amenaza	Control	
[A] Ataques intencionados	[A.9] [Re-]encaminamiento de mensajes	13.1.2	Seguridad de los servicios de red
[A] Ataques intencionados	[E.1] Errores de los usuarios	7.2.2	Toma de conciencia, capacitación y formación en la seguridad de la información
[E] Errores y fallos no intencionados	[E.10] Errores de secuencia	13.2.2	Acuerdos sobre transferencia de información
[E] Errores y fallos no intencionados	[E.15] Alteración accidental de la información	12.3.1	Respaldo de la información
[E] Errores y fallos no intencionados	[E.18] Destrucción de información	12.3.1	Respaldo de la información
[E] Errores y fallos no intencionados	[E.19] Fugas de información	9.4.1	Restricción de acceso a la información
[E] Errores y fallos no intencionados	[E.2] Errores del administrador	12.4.3	Registros del administrador y del operador
[E] Errores y fallos no intencionados	[E.20] Vulnerabilidades de los programas (software)	12.2.1	Controles contra códigos maliciosos
[E] Errores y fallos no intencionados	[E.21] Errores de mantenimiento / actualización de programas (software)	12.1.2	Gestión de cambios
[E] Errores y fallos no intencionados	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	12.1.2	Gestión de cambios
[E] Errores y fallos no intencionados	[E.24] Caída del sistema por agotamiento de recursos	11.2.2	Servicios de suministro
[E] Errores y fallos no intencionados	[E.25] Pérdida de equipos	11.2.6	Seguridad de equipos y activos fuera de las instalaciones
[E] Errores y fallos no intencionados	[E.28] Indisponibilidad del personal	6.1.2	Segregación de deberes
[E] Errores y fallos no intencionados	[E.4] Errores de configuración	12.4.3	Registros del administrador y del operador
[E] Errores y fallos no intencionados	[E.8] Difusión de software dañino	12.2.1	Controles contra códigos maliciosos
[E] Errores y fallos no intencionados	[E.9] Errores de [re-]encaminamiento	13.1.2	Seguridad de los servicios de red
[E] Errores y fallos no intencionados	[I.*] Desastres industriales	11.1.4	Protección contra amenazas externas y ambientales
[I] De origen industrial	[I.1] Fuego	11.1.4	Protección contra amenazas externas y ambientales
[I] De origen industrial	[I.10] Degradación de los soportes de almacenamiento de la información	11.2.4	Mantenimiento de equipos
[I] De origen industrial	[I.11] Emanaciones electromagnéticas	11.1.4	Protección contra amenazas externas y ambientales
[I] De origen industrial	[I.2] Daños por agua	11.1.4	Protección contra amenazas externas y ambientales

Cuadro 27. (Continuación)

Tipo de amenaza	Amenaza	Control	
[I] De origen industrial	[I.3] Contaminación mecánica	11.1.4	Protección contra amenazas externas y ambientales
[I] De origen industrial	[I.4] Contaminación electromagnética	11.1.4	Protección contra amenazas externas y ambientales
[I] De origen industrial	[I.5] Avería de origen físico o lógico	11.2.4	Mantenimiento de equipos
[I] De origen industrial	[I.6] Corte del suministro eléctrico	11.2.2	Servicios de suministro
[I] De origen industrial	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4	Protección contra amenazas externas y ambientales
[I] De origen industrial	[I.8] Fallo de servicios de comunicaciones	13.1.1	Controles de redes
[I] De origen industrial	[I.9] Interrupción de otros servicios y suministros esenciales	17.2.1	Disponibilidad de instalaciones de procesamiento de información
[I] De origen industrial	[N.*] Desastres naturales(CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN)	17.2.1	Disponibilidad de instalaciones de procesamiento de información
[N] Desastres naturales	[N.1] Fuego	11.1.4	Protección contra amenazas externas y ambientales
[N] Desastres naturales	[N.2] Daños por agua	11.1.4	Protección contra amenazas externas y ambientales
Fuente: autores			

7.6 EVALUACIÓN DE MADUREZ MÉDERI

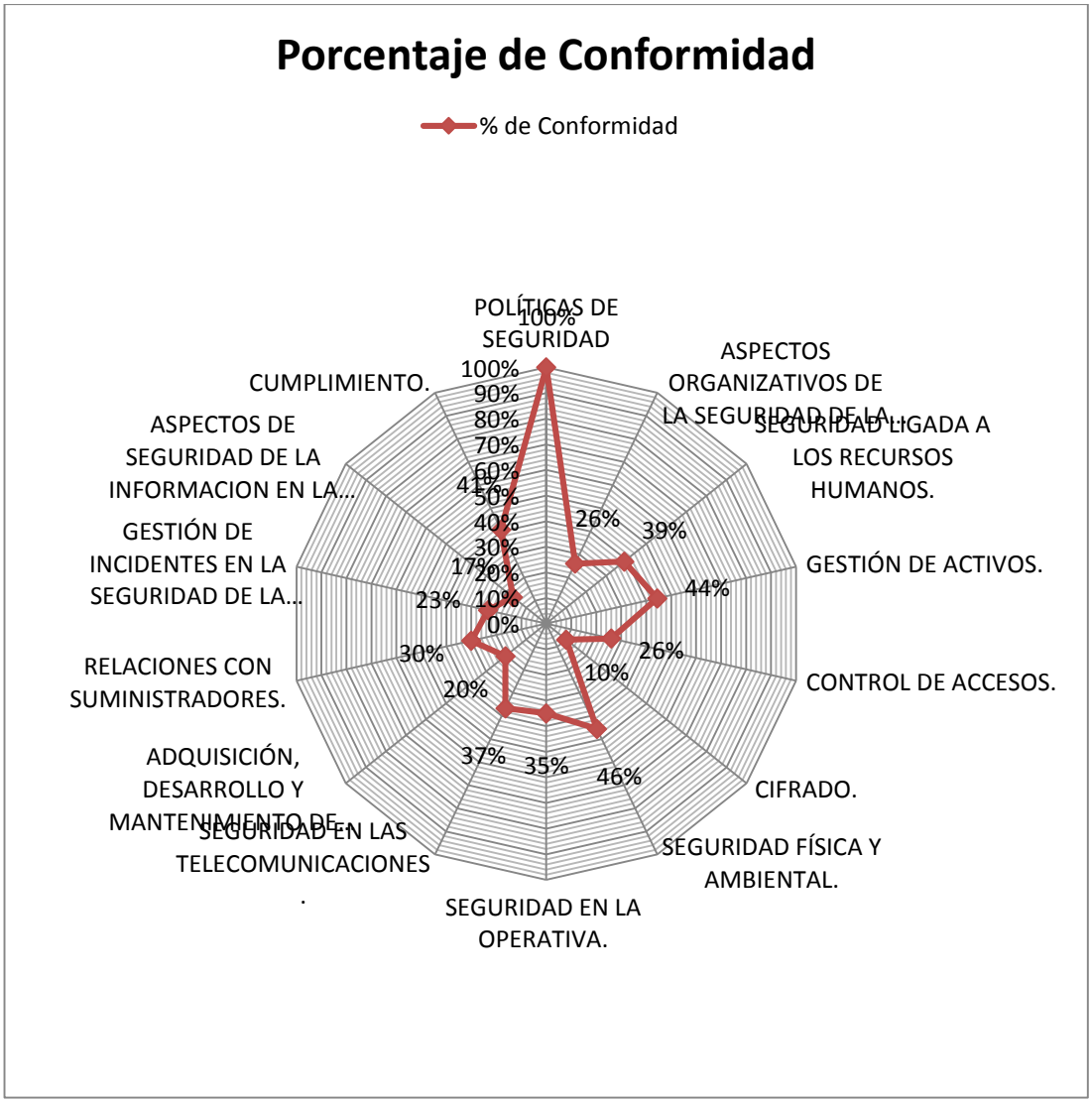
Con la evaluación de Madurez de los ocho dominios de seguridad de la norma ISO: 27002 se observan porcentajes muy bajos de conformidad de los dominios, uno de estos es el de aspectos de seguridad de la información en la gestión de la continuidad del negocio que tiene una conformidad del 17%, dejando evidenciado, que se tienen pocos controles implementados en la institución para mitigar si se llegara a presentar algún evento que afecte el desarrollo de las actividades de la institución incluyendo al funcionamiento del sistema de información se puede ver el análisis en el anexo E**.** (Ver cuadro 28)

Cuadro 18. Evaluación de Madurez respecto a los controles definidos en la ISO 27002:2013.

	Dominio	Porcentaje de Conformidad	No Conformidad Mayor	No Conformidad Menor	Observación
A.5	Políticas de seguridad	100%	0	0	2
A.6	Aspectos organizativos de la seguridad de la información.	26%	5	2	0
A.7	Seguridad ligada a los recursos humanos.	39%	2	4	0
A.8	Gestión de activos.	44%	2	8	0
A.9	Control de accesos.	26%	10	4	0
A.10	Cifrado.	10%	2	0	0
A.11	Seguridad física y ambiental.	46%	3	12	0
A.12	Seguridad en la operativa.	35%	8	6	0
A.13	Seguridad en las telecomunicaciones.	37%	3	4	0
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	20%	10	3	0
A.15	Relaciones con suministradores.	30%	3	2	0
A.16	Gestión de incidentes en la seguridad de la información.	23%	6	1	0
A.17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	17%	3	1	0
A.18	Cumplimiento.	41%	3	5	0
Fuente: autores					

Para ver el porcentaje de conformidad de controles implementados en la institución se puede dimensionar. (Ver gráfica 1).

Gráfica 1. Porcentaje de conformidad con respecto a los dominios de la ISO 27002:2013.



Fuente: autores

7.7 ESTIMACIÓN DEL IMPACTO

Para el cálculo del impacto se toman todos los activos y su valoración cuantitativa valorada por cada uno de los dominios DICAT, se toma el valor máximo de la frecuencia con la que puede ocurrir y el valor máximo del impacto por cada uno de los dominios y se realiza el cálculo del impacto potencial, realizando la multiplicación del valor del activo por el impacto, teniendo como resultado la columna impacto potencial de los activos. (Ver cuadro 29)

Cuadro 19. Calculo del Impacto potencial del activo.

Impacto Potencial = Valor Del Activo * Impacto

Activos		Valor	Criterios de valoración cuantitativa de los activos					Frecuencia	Impacto sobre la dimensión del activo					Impacto potencial del activo				
			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad		Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Activos Esenciales																		
INFO	[INFO] Historias Clínicas-Administrativa	MA Muy Alta	10	10	10	10	10											
[SW] Aplicaciones / Software																		
SW1	Aplicación Servinte Clinical Suite Enterprise	MA Muy Alta	9	9	9	9	8	10	90%	80%	80%	80%	0%	8,1	7,2	7,2	7,2	0
SW2	SO (Sistemas Operativos)	MA Muy Alta	9	8	7	7	9	10	90%	80%	50%	0%	0%	8,1	6,4	3,5	0	0
[HW] Equipos informáticos (hardware)																		
HW1	Servidores de Aplicaciones	MA Muy Alta	8	5	8	6	6	10	100 %	90%	90%	75%	0%	8	4,5	7,2	4,5	0
HW2	Servidores de Componentes	MA Muy Alta	8	5	8	6		10	100 %	75%	90%	35%	0%	8	3,8	7,2	2,1	0
HW3	Servidor de directorio Activo	MA Muy Alta	9	5	7	6		1	100 %	85%	80%	60%	0%	9,0	4,25	5,6	3,6	0
HW4	Servidor de Integración Laboratorio	M Media	7	7	5	4		10	100 %	70%	70%	60%	0%	7	4,9	3,5	2,4	0
HW5	Servidor de Integración Imágenes DX	M Media	7	7	5	4		10	100 %	70%	70%	60%	0%	7	4,9	3,5	2,4	0

Cuadro 29. (Continuación)

Activos		Valor	Criterios de valoración cuantitativa de los activos					Frecuencia	Impacto sobre la dimensión del activo					Impacto potencial del activo				
			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad		Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
HW6	Servidor de Archivos PDF	A Alta	7	9	9	9	8	10	100 %	90%	95%	85%	0%	7,0	8,1	8,6	7,7	0
HW7	Servidor de Impresión Automática	M Media	7					10	100 %	50%	50%	20%	0%	7	0	0	0	0
HW8	Servidor de Impresión Manual	M Media	7					10	100 %	50%	50%	20%	0%	7	0	0	0	0
HW9	Servidor de Reportes	M Media	5	3	8	2	6	10	100 %	30%	85%	50%	0%	5	0,9	6,8	1	0
HW10	Servidor de Backup	A Alta	10	10	10	8	8	1	100 %	85%	90%	60%	0%	10	8,5	9	4,8	0
HW11	Estaciones de trabajo	B Baja	6	5	5	5	5	10	100 %	85%	85%	50%	0%	6	4,25	4,25	2,5	0
HW12	Servidor de Base de datos Informix	MA Muy Alta	10	9	10	9	9	10	100 %	100%	100%	90%	0%	10	9	10	8,1	0
[COM] Redes de comunicaciones																		
COM1	Switch, Rourter	A Alta	7	5	5	5	5	1	100%	75%	75%	0%	0%	7,0	3,8	3,8	0	0
COM2	Red Local	MA Muy Alta	9	7	9	9	7	1	100%	75%	75%	0%	0%	9	5,3	6,8	0	0
COM3	Fw Palo Alto	A Alta	9	9	9	9	7	0,1	100%	85%	90%	50%	0%	9,0	7,7	8,1	4,5	0
COM4	Controladora de Red	MA Muy Alta	9	9	9	8	8	1	100%	85%	90%	75%	0%	9	7,7	8,1	6	0
[AUX] Equipamiento auxiliar																		
AUX1	UPS	MA Muy Alta	10					1	100%	0%	0%	0%	0%	10	0	0	0	0
AUX2	Aire Acondicionado	A Alta	8					10	100%	0%	0%	0%	0%	8	0	0	0	0
AUX3	Controlador de Temperatura y Humedad	A Alta	8					0,1	100%	0%	0%	0%	0%	8	0	0	0	0
AUX4	control de acceso	A Alta	7					0,1	100%	0%	50%	0%	0%	7	0	0	0	0

Cuadro 29. (Continuación)

Activos		Valor	Criterios de valoración cuantitativa de los activos					Frecuencia	Impacto sobre la dimensión del activo					Impacto potencial del activo				
			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad		Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
[SS]Servicios Subcontratados																		
SS1	Conexión a Internet	M Media	8				6	1	100%	50%	80%	70%	60%	8	0	0	0	3,6
[L] Instalaciones																		
L1	Centro de Computo HUM	MA Muy Alta	10	10	8	8	9	0,01	100%	0%	0%	0%	0%	10	0	0	0	0
L1	Centro de Computo HUBU	A Alta	9	8	8	8	8	0,01	100%	0%	0%	0%	0%	9	0	0	0	0
[P] Personal																		
P1	Usuarios Funcionales	M Media	5					100	100%	85%	75%	75%	0%	5,0	0	0	0	0
P2	Jefe de Tecnología y Comunicaciones	M Media	9					10	100%	75%	75%	75%	0%	9,0	0	0	0	0
P3	Coordinador de Infraestructura	A Alta	9					10	100%	75%	75%	0%	0%	9,0	0	0	0	0
P4	Coordinador de Base de datos	A Alta	9					10	100%	95%	95%	0%	0%	9,0	0	0	0	0
P5	Coordinador de Seguridad de la Información	A Alta	8					10	100%	95%	95%	0%	0%	8,0	0	0	0	0
P6	DBA	A Alta	9					10	100%	95%	95%	0%	0%	9,0	0	0	0	0
P7	Ingenieros de Base de datos	A Alta	9					10	100%	95%	95%	0%	0%	9,0	0	0	0	0
P8	Ingeniero de Imágenes Diagnosticas	M Media	7					10	100%	95%	95%	0%	0%	7,0	0	0	0	0

Cuadro 29. (Continuación)

Activos		Valor	Criterios de valoración cuantitativa de los activos					Frecuencia	Impacto sobre la dimensión del activo					Impacto potencial del activo				
			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad		Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
P9	Analista de data Center	A Alta	9					10	100%	75%	75%	0%	0%	9,0	0	0	0	0
P10	Técnicos de soporte	M Media	5					10	100%	75%	75%	0%	0%	5,0	0	0	0	0
P11	Jefe de enfermería de historia Clínica	M Media	8					10	95%	95%	95%	0%	0%	7,6	0	0	0	0
P12	Auxiliares de soporte Clínico	M Media	8					10	95%	95%	95%	0%	0%	7,6	0	0	0	0

Fuente: autores

7.8 ESTIMACIÓN DEL RIESGO POTENCIAL

Se evidencia que de acuerdo a la valoración de los activos al afectarse en su funcionalidad afecta considerablemente en las cinco dimensiones de seguridad reflejando en el cuadro Valoración del Riesgo, de acuerdo al análisis y la valoración calculada se definió que el valor de los riesgos con valores entre 100 y 81 se clasificaran como alto, entre 80 y 70 se clasificaran como alto, entre 69 y 50 se clasificaran como medio y menores de 49 se clasificaran como bajos, definidos por la probabilidad contra el impacto. (Ver cuadro 30)

Cuadro 30. Valoración del Riesgo

Riesgo	Impacto				
Probabilidad	MB Muy baja	B Baja	M Media	A Alta	MA Muy alta
MA: muy alto	A(80-70)	MA (100-81)	MA (100-81)	MA (100-81)	MA (100-81)
A: alto	M (69-50)	A(80-70)	A(80-70)	MA (100-81)	MA (100-81)
M: medio	B(<49)	M (69-50)	M (69-50)	A(80-70)	A(80-70)
B: bajo	B(<49)	B(<49)	B(<49)	M (69-50)	M (69-50)
MB: muy bajo	B(<49)	B(<49)	B(<49)	B(<49)	B(<49)

Fuente: Tabla Estimación del Riesgo - Metodología de Análisis y Gestión de riesgos de los sistemas de información Libro 3 - Método Pag.7

Para el cálculo del valor del riesgo potencial se toman, los activos con su respectiva valoración por dimensiones, tomando los valores máximos de la frecuencia, impacto del activo, el resultado del cálculo del impacto potencial del activo, se aplica la formula frecuencia por impacto potencial, obteniendo como resultado la columna de riesgo acumulado. (Ver cuadro 31)

Cuadro 31. Calculo del Riesgo Potencial de los activos.

Riesgo Potencial = Frecuencia * Impacto Potencial

Activos		Valor	Criterios de valoración cuantitativa de los activos					Frecuencia	Impacto sobre la dimensión del activo					Impacto potencial del activo					Riesgo potencial				
			Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad		Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad
Activos Esenciales																							
INFO	[INFO] Historias Clínicas-Administrativa	MA Muy Alta	10	10	10	10	10																
[SW] Aplicaciones / Software																							
SW1	Aplicación Servinte Clinical Suite Enterprise	MA Muy Alta	9	9	9	9	8	10	90%	80%	80%	80%	0%	8,1	7,2	7,2	7,2	0	81	72	72	72	0
SW2	SO (Sistemas Operativos)	MA Muy Alta	9	8	7	7	9	10	90%	80%	50%	0%	0%	8,1	6,4	3,5	0	0	81	64	35	0	0
[HW] Equipos informáticos (hardware)																							
HW1	Servidores de Aplicaciones	MA Muy Alta	9	5	8	6	6	10	100%	90%	90%	75%	0%	9	6,3	8,1	4,5	0	90	63	81	45	0
HW2	Servidores de Componentes	MA Muy Alta	9	5	8	6		10	100%	75%	90%	35%	0%	9	5,3	8,1	2,1	0	90	52,5	81	21	0
HW3	Servidor de directorio Activo	MA Muy Alta	9	5	7	6		1	100%	85%	80%	60%	0%	9,0	4,25	5,6	3,6	0	9	4,25	5,6	3,6	0
HW4	Servidor de Integración Laboratorio	M Media	9	7	5	4		10	100%	90%	70%	60%	0%	9	4,9	3,5	2,4	0	90	49	35	24	0
HW5	Servidor de Integración Imágenes DX	M Media	9	7	5	4		10	100%	90%	70%	60%	0%	9	4,9	3,5	2,4	0	90	49	35	24	0
HW6	Servidor de Archivos PDF	A Alta	9	9	9	9	8	10	100%	90%	95%	85%	0%	9,0	8,1	8,6	7,7	0	90	81	85,5	76,5	0

Cuadro 31. (Continuación)

Activos		Valor	Criterios de valoración cuantitativa de los activos					Frecuencia	Impacto sobre la dimensión del activo					Impacto potencial del activo					Riesgo potencial				
			Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad		Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad
HW7	Servidor de Impresión Automática	M Media	8					10	100%	50%	50%	20%	0%	7	0	0	0	0	80	0	0	0	0
HW8	Servidor de Impresión Manual	M Media	7					10	100%	50%	50%	20%	0%	7	0	0	0	0	70	0	0	0	0
HW9	Servidor de Reportes	M Media	5	3	8	2	6	10	100%	30%	85%	50%	0%	5	0,9	6,8	1	0	50	9	68	10	0
HW10	Servidor de Backup	A Alta	10	10	10	8	8	1	100%	85%	90%	60%	0%	10	8,5	9	4,8	0	10	8,5	9	4,8	0
HW11	Estaciones de trabajo	B Baja	6	5	5	5	5	10	100%	85%	85%	50%	0%	6	4,25	4,25	2,5	0	60	42,5	42,5	25	0
HW12	Servidor de Base de datos Informix	MA Muy Alta	10	9	10	9	9	10	100%	100 %	100%	90%	0%	10	9	10	8,1	0	100	90	100	81	0
[COM] Redes de comunicaciones																							
COM1	Switch, Rourter	A Alta	7	5	5	5	5	1	100%	75%	75%	0%	0%	7,0	3,8	3,8	0	0	7	3,75	3,75	0	0
COM2	Red Local	MA Muy Alta	9	7	9	9	7	1	100%	75%	75%	0%	0%	9	5,3	6,8	0	0	9	5,25	6,75	0	0
COM3	Fw Palo Alto	A Alta	9	9	9	9	7	0,1	100%	85%	90%	50%	0%	9,0	7,7	8,1	4,5	0	0,9	0,765	0,81	0,45	0
COM4	Controladora de Red	MA Muy Alta	9	9	9	8	8	1	100%	85%	90%	75%	0%	9	7,7	8,1	6	0	9	7,65	8,1	6	0
[AUX] Equipamiento auxiliar																							
AUX1	UPS	MA Muy Alta	10					1	100%	0%	0%	0%	0%	10	0	0	0	0	10	0	0	0	0
AUX2	Aire Acondicionado	A Alta	8					10	100%	0%	0%	0%	0%	8	0	0	0	0	80	0	0	0	0
AUX3	Controlador de Temperatura y Humedad	A Alta	8					0,1	100%	0%	0%	0%	0%	8	0	0	0	0	0,8	0	0	0	0
AUX4	control de acceso	A Alta	7					0,1	100%	0%	50%	0%	0%	7	0	0	0	0	0,7	0	0	0	0
[SS]Servicios Subcontratados																							
SS1	Conexión a Internet	M Media	8				6	1	100%	50%	80%	70%	60%	8	0	0	0	3,6	8	0	0	0	3,6
L1	Centro de Computo HUM	MA Muy Alta	10	10	8	8	9	0,01	100%	0%	0%	0%	0%	10	0	0	0	0	0,1	0	0	0	0
L1	Centro de Computo HUBU	A Alta	9	8	8	8	8	0,01	100%	0%	0%	0%	0%	9	0	0	0	0	0,09	0	0	0	0

Cuadro 31. (Continuación)

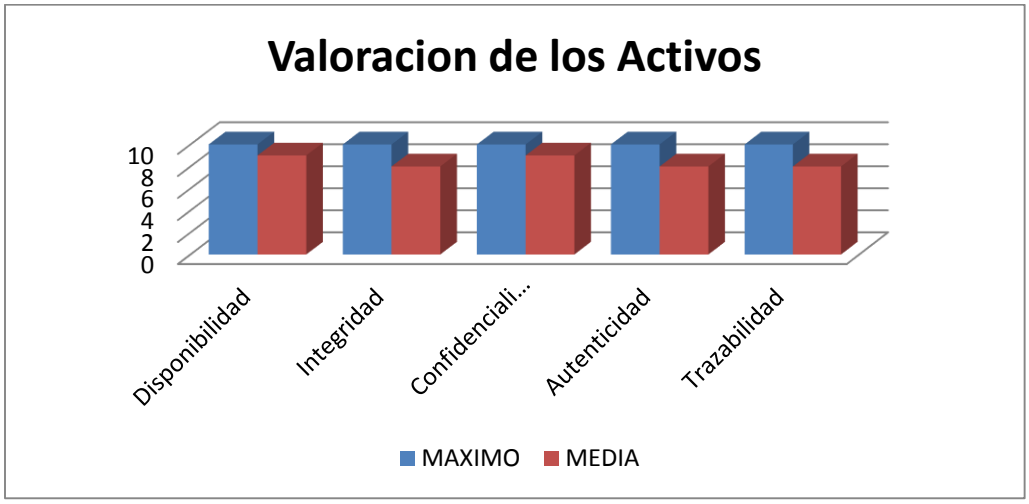
Activos		Valor	Criterios de valoración cuantitativa de los activos					Frecuencia	Impacto sobre la dimensión del activo					Impacto potencial del activo					Riesgo potencial				
			Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad		Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad	Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad
[L] Instalaciones																							
[P] Personal																							
P1	Usuarios Funcionales	M Media	5					100	100%	85%	75%	75%	0%	5,0	0	0	0	0	500	0	0	0	0
P2	Jefe de Tecnología y Comunicaciones	M Media	9					10	100%	75%	75%	75%	0%	9,0	0	0	0	0	90	0	0	0	0
P3	Coordinador de Infraestructura	A Alta	9					10	100%	75%	75%	0%	0%	9,0	0	0	0	0	90	0	0	0	0
P4	Coordinador de Base de datos	A Alta	9					10	100%	95%	95%	0%	0%	9,0	0	0	0	0	90	0	0	0	0
P5	Coordinador de Seguridad de la Información	A Alta	8					10	100%	95%	95%	0%	0%	8,0	0	0	0	0	80	0	0	0	0
P6	DBA	A Alta	9					10	100%	95%	95%	0%	0%	9,0	0	0	0	0	90	0	0	0	0
P7	Ingenieros de Base de datos	A Alta	9					10	100%	95%	95%	0%	0%	9,0	0	0	0	0	90	0	0	0	0
P8	Ingeniero de Imágenes Diagnosticas	M Media	7					10	100%	95%	95%	0%	0%	7,0	0	0	0	0	70	0	0	0	0
P9	Analista de data Center	A Alta	9					10	100%	75%	75%	0%	0%	9,0	0	0	0	0	90	0	0	0	0
P10	Técnicos de soporte	M Media	5					10	100%	75%	75%	0%	0%	5,0	0	0	0	0	50	0	0	0	0
P11	Jefe de enfermería de historia Clínica	M Media	8					10	95%	95%	95%	0%	0%	7,6	0	0	0	0	76	0	0	0	0
P12	Auxiliares de soporte Clínico	M Media	8					10	95%	95%	95%	0%	0%	7,6	0	0	0	0	76,0	0	0	0	0

Fuente: autores

7.9 ESTADO DEL RIESGO

Una vez terminado el análisis del riesgos realizando la validación del proceso y con la valoración realizada a cada uno de los activos por cada uno de los 5 dominios su valor máximo es 10 y la media está entre 8 y 9, indicando que los activos si son explotadas alguna de sus amenazas, se afectara la operación del hospital teniendo en cuenta que Servinte es una de las herramientas principales para el desempeño de su actividad económica, como es la de prestación de servicios en salud, considerando que el riesgo es alto en las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y la trazabilidad. (Ver gráfica 2).

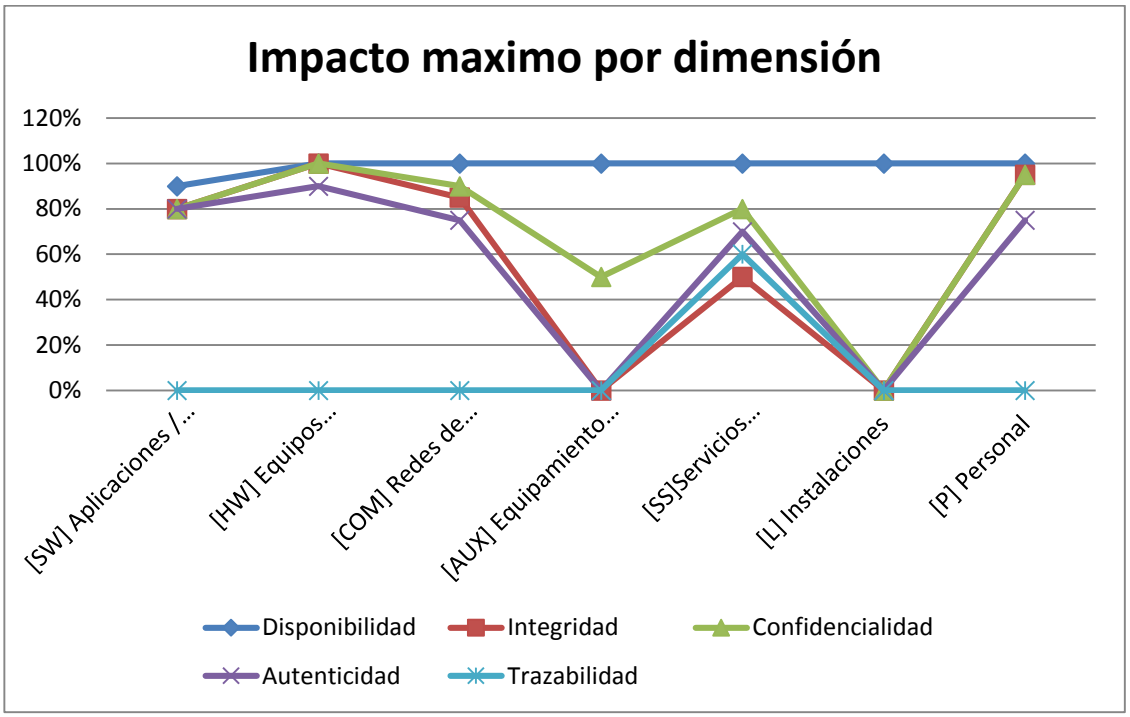
Gráfica 2. Valoración de los activos según DICAT.



Fuente: autores

En la gráfica 3 se puede observar como es el comportamiento del impacto por cada uno de los grupos de activos y es alto en la disponibilidad para casi todos los activos, la integridad, confidencialidad y autenticidad es alta en los activos que permiten la administración de la información como son el software, hardware y de comunicación evidenciando la importancia de plantear las estrategias de recuperación de estos activos, en cuanto al grupo de activos se evidencia que es el eslabón más débil ya que es el más complejo de controlar (Ver gráfica 3).

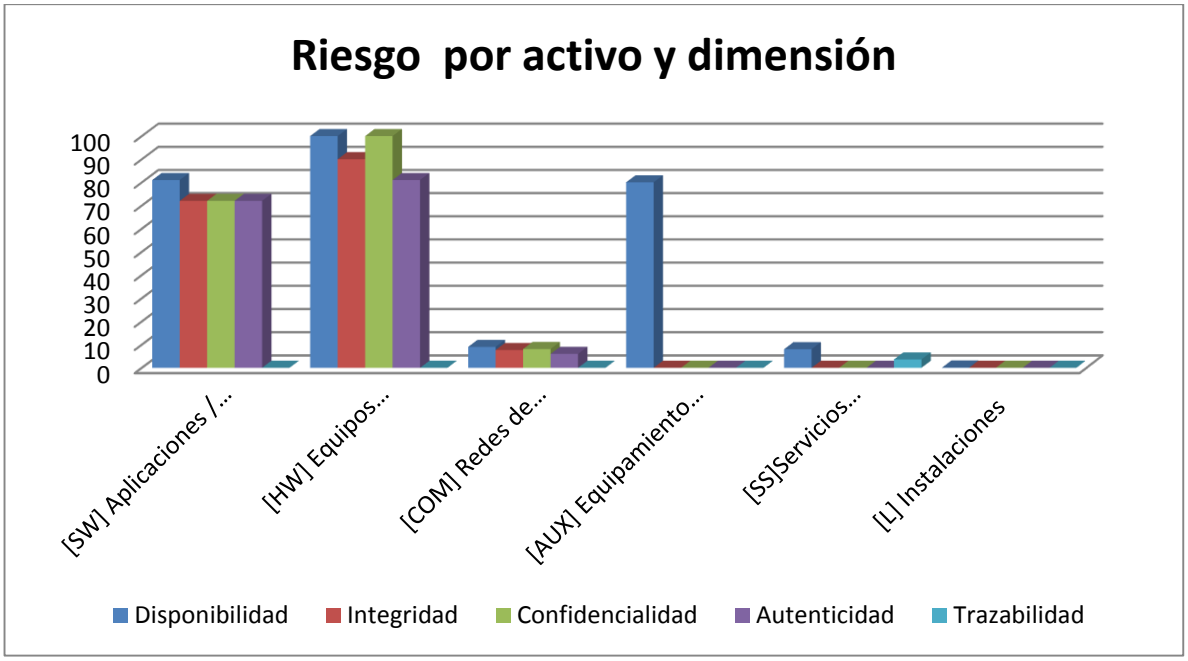
Gráfica3. Impacto máximo de los grupos de activos por dimensión



Fuente: autores

Después de identificar el impacto que tiene los activos en la institución frente a las posibles amenazas, se tiene la estimación del riesgo los activos que tiene mayor riesgo son las aplicaciones y equipos en los cuales hay que realizar los planes para mitigar los riesgos y que lleguen a tener valores de riesgo aceptable para la institución. (Ver gráfica 4)

Gráfica 4. Valoración del riesgo por dimensiones



Fuente: autores

En cuanto al grupo de activos de personal que se muestra en el cuadro, porque es uno de los activos en los cuales hay que realizar un mayor trabajo de concientización con los usuarios funcionales que son los de mayor impacto, nos genera en cuanto a la disponibilidad, integridad y confidencialidad en el manejo de la información sensible administrada por Servinte. (Ver cuadro 32)

Cuadro 32. Riesgo más alto.

Activo	Disponibilidad	Integridad	Cconfidencialidad	Autenticidad	Trazabilidad
[P] Personal	500	0	0	0	0
Fuente: autores					

Debido al tipo de información sensible con la cual trata la mayoría de procesos instituciones, se ve reflejado en el alto impacto y riesgo que presenta sus activos, si llegasen a explotar las vulnerabilidades que tiene los activos y que desencadene una no disponibilidad del sistema de información Servinte afectando la operatividad

institucional, reflejado se en la atención del paciente y pudiendo ocasionar como se dice en el argot hospitalario un evento adverso con el paciente ya que el personal debe contar con una alta disponibilidad de la información clínica y administrativa para prestar un óptimo servicio clínico.

Por eso la finalidad de este proyecto es plantear algunas estrategias con las cuales el proceso de tecnología de la Información y comunicación las evalué e implemente para así tener los planes de respuesta a los posibles eventos que puedan desplegar una recuperación de servicios institucionales. Teniendo en cuenta que este proceso de seguimiento, control y de mejora continua y que el proceso TIC es sobre quien recae esta responsabilidad.

8. ESTRATEGIAS DE RECUPERACIÓN

De acuerdo a los riesgos obtenidos y mediante el estudio y el planeamiento de estrategias se proyectó establecer mecanismos, procesos y procedimientos los cuales garanticen el restablecimiento de las operaciones y regresar a la normalidad de los procesos y activos críticos de negocio relacionados con el sistema Servinte, identificados mediante el análisis de impacto de negocio, la evaluación de madurez y el análisis de riesgos.

El proceso de Tecnología de la Información y Comunicación dentro de su planeación ha adelantado un proceso de actualización de su infraestructura tecnológica que le ha permitido adquirir componentes tecnológicos actuales que soporte las transacciones operativas que requieren los diferentes sistemas de información que son usados en la institución en su datacenter principal que está ubicado en la sede Mayor. De esta manera dimensionando la necesidad de implementar un centro de datos alterno que está ubicado en la sede en Barrios Unidos con las mismas características tecnológicas con las que cuenta el datacenter principal de Mayor, para soportar las necesidades tecnológicas requeridas para el funcionamiento del sistema de información Servinte. Este datacenter alterno se encuentra en alta disponibilidad ya que se ha dispuesto que algunos procesos de la sede en Barrios Unidos realicen las operaciones conectados a los servidores configurados en esta infraestructura, de esta manera asegurando que los componentes tecnológicos para el funcionamiento de Servinte, están en óptimo funcionamiento, en el momento de un despliegue del plan de recuperación. Se cuenta con dos réplicas de la base de datos, una se encuentra en Medellín con el proveedor UNE, la cual se tiene la disponibilidad de esta en el momento que sea necesario y la segunda replica está en el datacenter de HUBU que es la primera opción de pasar de ser replica a transaccional para el despliegue del plan de recuperación.

8.1 OBJETIVOS

- Planificar una respuesta a las posibles interrupciones, fallas o desastres mayores en el servicio relacionado con sistema Servinte y los cuales puedan generar indisponibilidad de los procesos críticos del hospital Méderi y su sede en barrios unidos.

- Establecer estrategias de recuperación del sistema de información Servinte, infraestructura tecnológica y personal involucrado, que lo soporta en caso de interrupción parcial o total del servicio.

- Definir la secuencia de actividades que se llevarán a cabo para comunicar un incidente, activar el plan de recuperación de destares, ponerlo en marcha y regresar al estado normal.

- Formalizar los criterios o condiciones que se deben cumplir para la toma de decisiones antes, durante y después de la ocurrencia de un incidente.

8.2 ALCANCE

El alcance de la estrategia está definido para los procesos críticos definidos en este plan de recuperación de desastres en el apartado BIA sistema de información Servinte, tabla 8. Procesos críticos identificados, los cuales son soportados por el sistema Servinte y la infraestructura tecnológica relacionada como crítica.

8.3 PRIORIDAD DE RECUPERACIÓN

La prioridad para realizar la recuperación de cada uno de los procesos se da de acuerdo a la calificación y análisis realizado en el tiempo objetivo de recuperación (RTO) identificado en el BIA. (Ver cuadro 33)

Cuadro 33. Prioridad de recuperación

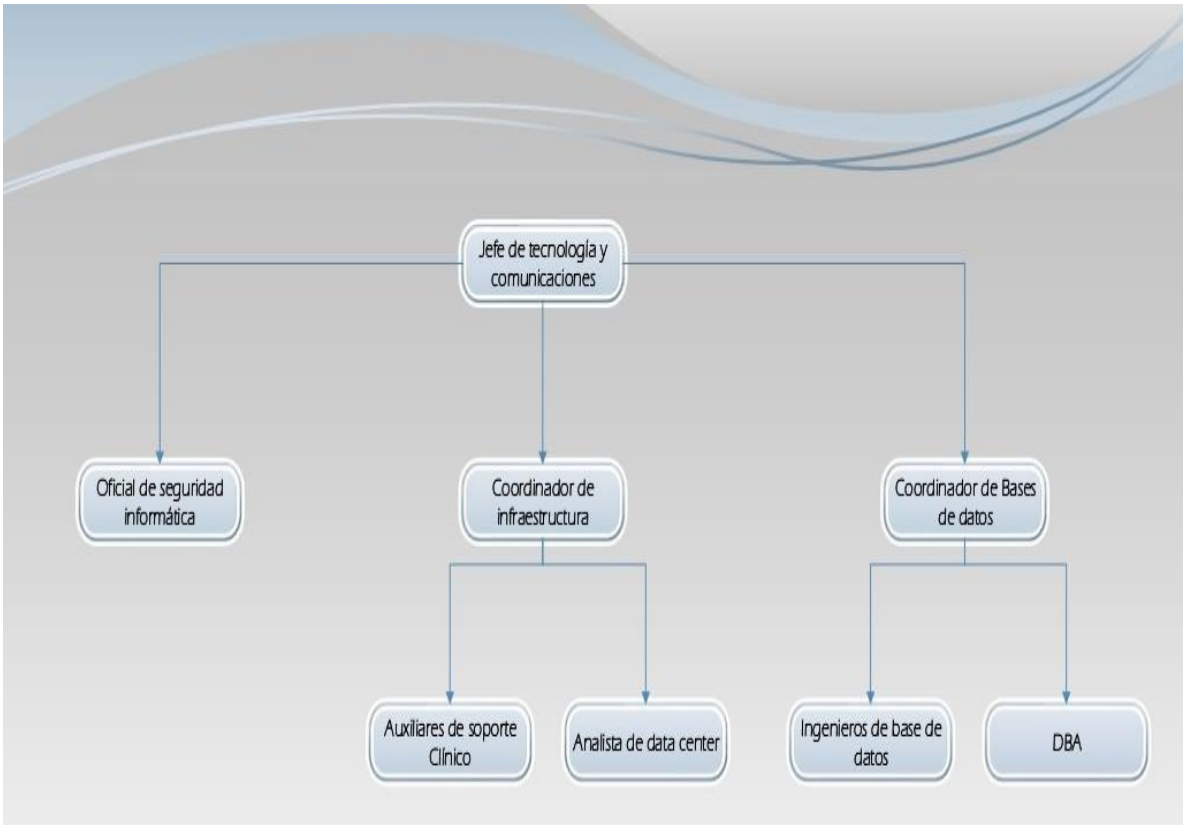
Proceso	Tiempo objetivo de recuperación
Urgencias	1
Enfermería	1
Cuidado critico	1
Servicio farmacéutico	1
Admisiones y autorizaciones	1
Imágenes diagnosticas	1
Laboratorio clínico y servicio transfusional	1
Tecnología de la información y comunicaciones	1
Clínicas medicas	2
Salud sexual y reproductiva	3
Logística y suministros	3
Tesorería	3
Programas especiales	4
Facturación	4
Atención al usuario	4
Inteligencia de negocios	4
Nutrición	5
Auditoría médica	5
Referencia y contra referencia	6
Cartera	7
Fuente: autores	

8.4 EQUIPO DE RECUPERACIÓN

Está conformado por el Especialista de Proyectos de Producción de Sistemas de información, el Especialista Centros de Cómputo y Comunicaciones, el Oficial de Seguridad de la Información y el personal técnico operativo (proveedor) que bajo la coordinación y orientación de los diferentes líderes, estarán en la capacidad de recuperar los sistemas de información y los componentes de TI críticos afectados luego de la materialización de un escenario de interrupción, teniendo en cuenta la secuencia de recuperación y la información básica requerida por cada sistema de información. Además, están los líderes de respuesta a emergencias, comunicaciones, jurídicos, soporte administrativo, transportes, entre otros.

8.4.1 Organigrama. Los roles y responsabilidades del equipo de recuperación serán ejercidos de acuerdo al organigrama. (Ver figura 3)

Figura 3. Organigrama equipo de recuperación.



Fuente: autores

8.4.1.1 Roles y responsabilidades

- Jefe de Tecnología y Comunicaciones:

o Comunicar a los directivos la situación del plan de recuperación.

o Comunicar a los jefes y coordinadores la activación del plan de recuperación y así dar inicio a los planes de contingencia definidos por cada uno de los procesos, mientras se realiza el proceso de recuperación en el datacenter alterno.

o Evaluar el impacto que se genera el plan de recuperación.

- Coordinador de Infraestructura:

o Verificación del correcto funcionamiento de los centros de datos principal y alterno antes, durante y después del plan de recuperación e informar oportunamente si se presenta alguna variación significativa que pueda poner en riesgo la operación.

o Verificar de manera periódica las diferentes conexiones con el centro de datos, canales dedicados entre sedes, así como con el centro de datos externo.

o Validar con los proveedores de los servicios de comunicación, protección para el adecuado funcionamiento de los mismos.

o Coordinar su equipo de apoyo para realizar las actividades de recuperación y de contingencia que se han establecido el plan de recuperación.

o Hacer periódicamente pruebas de recuperación de las bases de datos respaldadas previamente de acuerdo a lo definido en los Procedimientos de Respaldo y Restauración de Copias.

o Coordinar las acciones definidas en conjunto con el Coordinador de Base de datos y su personal de apoyo para el desarrollo de las actividades del plan de recuperación hasta retornar a la operación normal.

- Coordinador de Base de datos

o Establecer la comunicación con el DBA de la base de datos, cuando se despliegue el plan de recuperación.

o Coordinar el equipo de trabajo para realizar el proceso de recuperación según planeación establecida.

o Coordinar los procesos de verificación cuando corresponda el acceso a las aplicaciones en el momento en que se dé inicio la recuperación de bases de datos del sistema de información.

o Coordinar las actividades necesarias en conjunto con el coordinador de infraestructura y el personal de apoyo respectivo, para el desarrollo de las actividades del plan de restauración hasta retornar a la operación normal.

- Coordinador de Seguridad de la Información:

o Monitorear y asegurar el cumplimiento del plan de recuperación.

o Realizar recomendaciones para mejorar actividades y procesos que permitan minimizar los riesgos de operación.

o Realizar informes de las causas del inicio del plan de recuperación y del restablecimiento de las operaciones a la normalidad, de acuerdo al seguimiento dado por las coordinaciones de base de datos e infraestructura.

- DBA:

o Monitoreo de la disponibilidad funcionamiento de la base de datos.

o Dar soporte de los posibles inconvenientes que se presenten con la base de datos.

o Realizar las respectivas operaciones para optimizar el funcionamiento de la base de datos.

o Administrar los servidores de base de datos.

- Analista del Data Center:

o Realizar las configuraciones respectivas para la generación automática de las copias de respaldo de los diferentes sistemas de información, así como sus bases de datos.

o Verificar que las copias de respaldo programadas se hayan ejecutado y terminado correctamente.

o Tener a disposición las copias de respaldo.

o Dar disponibilidad de recursos de espacio al DBA para la restauración de copias de seguridad.

- Ingenieros de Base de datos:

o Realizar un diagnóstico preliminar de incidente y comunicarlo a los coordinadores.

o Verificar la configuración de los servidores.

o Verificar la configuración de instalación de la aplicación para su correcto funcionamiento.

o Verificar que los servicios de los servidores de integraciones, impresión están corriendo.

o Dar soporte a los usuarios con los posibles errores que se presente con el sistema de información.

- Jefe de Enfermería Clínica:

o Verificación de los maestros de configuración de Servinte.

o Realizar las pruebas de funcionamiento de la aplicación al estar disponible

o Dar soporte a los usuarios al momento que el sistema esté disponible

- Auxiliares de soporte Clínico:

o Realizar las pruebas de funcionamiento de la aplicación al estar disponible.

o Dar soporte a los usuarios al momento que el sistema esté disponible.

8.4.1.2 Roles Alternos. De acuerdo al análisis de riesgos se evidencio que el personal es uno de los riesgos con mayor calificación, en el momento de activación del DRP puede darse el caso que alguno de los responsables del equipo de recuperación no se encuentre disponible, por tal motivo se define el cargo alterno que pueda suplir el rol requerido. (Ver cuadro 34)

Cuadro 34. Cargos alternos

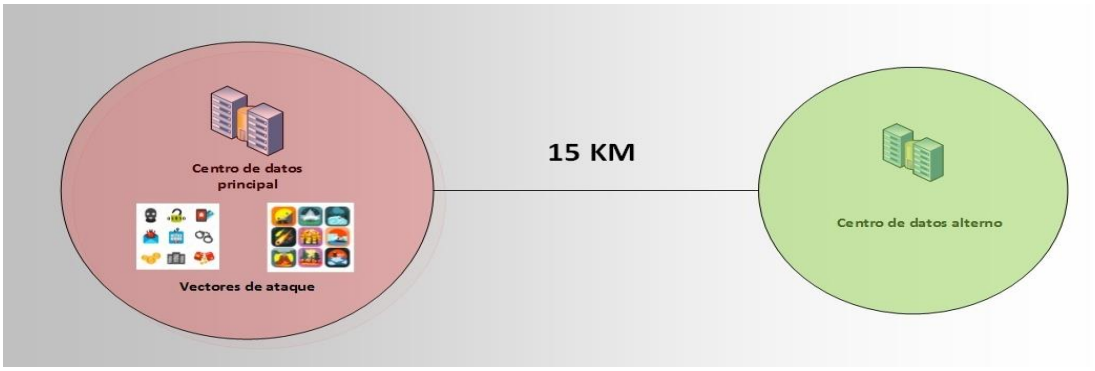
Cargo Principal	Cargo alterno
Jefe de tecnología y comunicaciones	Coordinador de base de datos
Coordinador de infraestructura	Analista del data center
Coordinador de base de datos	Ingeniero de base de datos
Coordinador de seguridad de la información	Jefe de tecnología y comunicaciones
Administrador de base de datos	Administrador de base de datos
Analista del data center	Ingeniero de Imágenes diagnosticas
Ingenieros de base de datos	Ingenieros de base de datos
Auxiliares de soporte clínico	Auxiliares de soporte clínico
Fuente: autores	

8.5 ESTRATEGIA AFECTACIÓN TOTAL DE SERVINTE - CENTRO DE DATOS ALTERNO

Esta estrategia se tendrá que activar cuando los activos de información definidos como críticos, resulten inoperativos por causa de un desastre y por ende se afecten alguno de los procesos de impacto crítico, teniendo en cuenta la prioridad de recuperación.

Dicho centro de datos se tendrá que encontrar ubicado a una distancia aislada no menor a 15 Kilómetros a la redonda del sitio principal, garantizando que una catástrofe natural, atentado terrorista, tecnológico, etc. Que se pueda materializar en la ubicación geográfica del centro de datos principal, no llegue a afectar también el centro de datos alterno. (Ver figura 4)

Figura 4. Ubicación del centro de datos alterno



Fuente: autores

8.5.1 Identificación de recursos en el centro de datos alterno. El sistema de información Servinte está diseñada con una arquitectura cliente servidor, este diseño está basado en la distribución del procesamiento entre los equipos servidores y los equipos clientes, permitiendo centralizar la administración de la información y la segregación de responsabilidades. (Ver cuadro 35)

- Redes y comunicaciones: Para la apropiada interconexión al centro de datos alterno deberá contar con:

Canal de datos de 16 Mbps IP Capa II, dedicado sin rehusó, lineal entre la Sede Principal del hospital Méderi y el Sitio Alterno de Datos, la última milla en fibra óptica y enrutamiento en los dos extremos.

Servicio de Internet Banda Ancha de 4 Mbps para los servidores aprovisionados en el Sitio Alterno de Datos. Esto es requerido para las conexiones que soportaran el acceso al sistema Servinte.

Switch administrable, distribución de conexión entre dispositivos

Estos elementos deberán contar con una escalabilidad del 100%

Cuadro 35. Equipamiento redes y telecomunicaciones

Redes y comunicaciones	Características
Canal de datos	16 Mbps dedicado
Canal de internet	4 Mbps dedicado
Switch	Equiparable a principal
Firewall Palo Alto	Equiparable a principal
Fuente: autores	

- Servidores. El número de servidores serán utilizados según la cantidad de los mismos que sean requeridos por cada uno de los procesos definidos en el BIA, así: (Ver cuadro 36)

Cuadro 36. Equipamiento servidores.

Nivel	Usua-rios	Servidor aplicaciones	Servidor de componentes	Servidor de impresión	Servidor pdf	Servidor de integración de imágenes diagnosticas	Servidor de integración de laboratorio	Servi-dor de repor-tes	Servidor de base de datos	Servidor de backup	Servidor de dominio
Crítico 1	314	15	6	1*	1*	1*	1*	1*	1*	1*	1*
Crítico 2	208	8	2	1*	1*	0	0	0	1*	1*	1*
Alto 3	30	2	1	1*	1*	0	0	1*	1*	1*	1*
Moderado 4	78	5	2	1*	1*	0	0	1*	1*	1*	1*
Moderado 5	59	2	1	1*	0	0	0	1*	1*	1*	1*
Bajo 6	5	1	0	0	0	0	0	0	1*	1*	1*
Bajo 7	12	0	1	1*	0	0	0	1*	1*	1*	1*
Total	706	33	13	1	1	1	1	1	1	1	1

Fuente autores

8.5.2. Base de datos y Software. Para la adecuada recuperación de los procesos críticos establecidos es necesario contar con el software definido, los cuales soportaran cada una de las necesidades en cuanto a funcionalidad del software Servinte. (Ver cuadro 37)

Cuadro 20. Identificación de software necesario

Ítem	Nombre
Base de datos	Informix
Aplicativos	Servinte
	Visor PDF
Aplicativo complementario	Razor
	Sql
	Agility
	Almera
	Mipres

Fuente: autores

- Informix: Motor de la base de datos

- Servinte: Aplicación que administra la información clínica y administrativa de la institución.

- Visor PDF: Permite visualizar la información en forma estructurada

- Razor: Administrador de conexión a la base datos para dar soporte a los usuarios en caso de presentar fallas con los datos de la base de datos.

- Agility: Aplicación que administra las imágenes diagnosticas que le son tomadas a los pacientes.

- Almera: Aplicación la cual permite reportar a los usuarios los inconvenientes que tengan con la aplicación y otras herramientas que se usan en la institución.

- Mipres: Aplicación gubernamental en la cual se deben generar los formatos no pos (Medicamentos y procedimientos controlados).

- *Equipamiento auxiliar*

El centro de datos alterno tendrá que cumplir con todos los estándares eléctricos referidos a protecciones, montajes, puestas a tierra y respaldos. Su funcionamiento estará respaldado con un sistema de suministro continuo (no interrumpido) de energía, regulada UPS en sistema redundante y con una planta diesel de 125KVA que lo complemente. Cuenta con circuitos independientes, protegidos por breakers para alimentaciones de fuentes DC, sistemas de alimentación comercial con sus protecciones respectivas, sistemas de puesta a tierra, temperatura ambiente controlada para el correcto funcionamiento de los equipos, protección contra la luz directa del sol.

Sistema de aire acondicionado regulado de temperatura, los equipos de aire acondicionado deberán ser monitoreados por el centro de control de seguridad, mediante la activación de alarmas luminosas y el registro de alarmas en log de eventos con notificación vía correo electrónico.

Los montajes deberán ser realizados bajo normas técnicas de cableado estructurado, contando entre otros, con ductos y bandejas porta cables, para la adecuada distribución de cables de alimentación y cables de señal. Los equipos de concentración tendrán redundancia en fuentes, lo cual brinda una alta confiabilidad.

Las instalaciones cumplen con estrictas normas de seguridad ambiental y física, para garantizar la protección del personal involucrado y la de los equipos. Se cuenta con vigilancia privada 7x24 en el edificio, cámaras de seguridad en el edificio, en el

interior del área administrativa y el Centro de Datos.

El ingreso al área administrativa se realizará por medio de lector biométrico. Todo el personal que ingrese deberá llenar una bitácora de ingreso y estar permanente acompañado de personal del Centro de Datos para realizar cualquier actividad.

Deberá con un circuito cerrado de televisión el cual almacene todos los eventos de las cámaras ubicadas estratégicamente en el mismo. (Ver tabla 2)

Tabla 2. Equipamiento auxiliar centro de datos alterno.

Equipamiento auxiliar
UPS Eléctrica
UPS Diesel
Aire Acondicionado
Controlador de temperatura y humedad
Control de acceso
Sistema detector de incendios
Sistema CCTV
Fuente: autores

8.5.3 Fases de recuperación. Para el desarrollo del plan de recuperación se identificó las siguientes 3 fases:

Fase 1: Planeación y puesta en marcha el centro de cómputo alterno de HUBU.

Fase 2: Recuperación y validación de procesos y aplicaciones en el centro de cómputo alterno de HUBU

Fase 3: Normalización de las operaciones al datacenter principal en el hospital mayor.

- Fase 1 Planeación y puesta en marcha el centro de cómputo alterno de HUBU

Se recibe el reporte generando un ticket. Los ingenieros de base de datos realizan la evaluación del caso y si es de su competencia seráasignado al personal responsable.

- Se realiza evaluación primaria del incidente y se ejecuta plan de comunicaciones, actividad a cargo del coordinador de infraestructura.

- Se activa el plan de recuperación por parte del jefe de tecnología y comunicaciones o quien haga sus veces.

- Organización de reunión de inicio del plan de recuperación con el equipo de recuperación, Actividad a cargo del Coordinador de Seguridad de información y la Jefe de Tecnología o quien haga sus veces

- Distribuir el personal que se dirigirá al centro de datos alterno de ser necesario.

- Se realiza diligenciamiento del reporte de indisponibilidad de servicio Servinte Anexo F. “Reporte de incidente Servinte”, actividad a cargo del jefe de tecnología y comunicaciones

- Realizar la configuración necesaria para que los equipos puedan iniciar los procesos del Hospital Mayor en el centro de datos alterno, actividad a cargo de los Coordinadores de infraestructura y de Base de datos o quien haga sus veces.

- Coordinar las comunicaciones con el personal que está a cargo del centro de cómputo alterno, actividad a cargo del Coordinador de Infraestructura o quien haga sus veces.

- Identificar con el personal encargado de la recuperación, los elementos críticos para su restablecimiento, según los roles y responsabilidades, actividad a cargo del Jefe de tecnología y comunicaciones o quien haga sus veces.

- Validación de la disponibilidad de la infraestructura para el proceso de recuperación del proceso crítico en el datacenter alterno, actividad a cargo del Coordinador de infraestructura o quien haga sus veces.

- Validar los componentes de hardware, software para el proceso de recuperación en el datacenter alterno, según línea base de los diferentes módulos de Servinte que se tiene en funcionamiento en ambiente de producción, actividad a cargo del Coordinador de infraestructura y el Coordinador de Base de datos o quienes haga sus veces.

- Verificar los servicios de terceros si se encuentran con la disponibilidad necesaria para iniciar el proceso de recuperación, actividad a cargo del Coordinador de infraestructura o quien haga sus veces.

- Validar y coordinar las actividades que son desarrolladas por colaboradores y proveedores para el desarrollo del plan de recuperación, actividad a cargo del Coordinador de seguridad de la información o quien haga sus veces.

- Notificar al DBA que se iniciara el proceso de recuperación, actividad a cargo del Coordinador de bases de datos o quien haga sus veces y según el plan de comunicaciones.

- Validar las pruebas de funcionalidad que cumplan con las necesidades de procesamiento necesario para la recuperación de los procesos críticos con los recursos del datacenter alterno, actividad a cargo del Coordinador de infraestructura con apoyo de auxiliares de data center y del coordinador de base de datos e ingenieros de base de datos o quienes haga sus veces.

- Fase 2: Recuperación y validación de procesos críticos y aplicaciones en el centro de cómputo alterno de HUBU

- Ubicar la base de datos de réplica como principal, actividad a cargo del DBA o quien haga sus veces.

- Validación del funcionamiento del motor de base de datos, actividad a cargo del DBA con apoyo de los ingenieros de bases de datos o quienes haga sus veces.

- Verificar el plan de restauración de los procesos críticos según la prioridad identificada, actividad a cargo del jefe de tecnología y comunicaciones con apoyo del coordinador de seguridad de la información.

- Verificación de los componentes tecnológicos para el funcionamiento del sistema de información servidores de (aplicaciones, componentes, Integraciones, impresiones, estaciones de trabajo), actividad liderada por el Coordinador de infraestructura y el coordinador de base de datos, con apoyo los auxiliares de soporte clínico y técnicos de soporte.

- Monitoreo constante de la disponibilidad de los recursos tecnológicos del datacenter alterno, actividad liderada por el coordinador de infraestructura con apoyo del coordinador de seguridad de la información, auxiliar del data center.

- Seguimiento a los recursos de comunicación entre las sedes, actividad a cargo de los ingenieros de bases de datos con apoyo de técnicos de soporte.

- Brindar el soporte técnico requerido a los usuarios internos y colaboradores, actividad a cargo de los técnicos de soporte.

- Seguimiento al desempeño de los recursos tecnológicos que soportan la recuperación de los procesos identificados como críticos, actividad a cargo del coordinador de seguridad de la información.

- Seguimiento y coordinación con los colaboradores que hacen uso del sistema de información tecnológica y las integraciones correspondientes, actividad liderada por

el jefe de tecnología y comunicaciones con apoyo del coordinador de seguridad de la información.

- Fase 3: Normalización de las operaciones

o Dimensionar el daño ocasionado por el incidente, actividad liderada por coordinador de seguridad de la información, con apoyo de coordinador de infraestructura, coordinador de base de datos, DBA.

o Valorar que recursos son necesarios para restablecer las operaciones al datacenter principal, actividad a cargo del coordinador de infraestructura.

o Planear el momento de restablecer los procesos en el datacenter principal, actividad a cargo del jefe de tecnología y comunicaciones.

o Definir en conjunto con el equipo de recuperación el tiempo indicado para restablecer a la normalidad las operaciones, actividad a cargo del jefe de tecnología y comunicaciones.

o Elaboración del informe del proceso de restauración a la normalidad de las operaciones en el datacenter principal, actividad a cargo del coordinador de infraestructura con apoyo del coordinador de seguridad de la información.

o Verificación de la infraestructura tecnológica del datacenter principal y componentes requeridos para la reanudación de las operaciones en el datacenter principal, actividad a cargo del coordinador de infraestructura con apoyo de auxiliares de data center

o Coordinar las actividades de restauración, actividad a cargo del jefe de tecnología y comunicaciones con apoyo del equipo de recuperación.

o Realizar backup de la base de datos de réplica para ejecutarla como principal, actividad a cargo del coordinador de base de datos con apoyo de los ingenieros de base de datos.

o Validar el proceso de restauración si ha sido óptimo con los recursos del datacenter principal, actividad a cargo del coordinador de infraestructura, coordinador de base de datos, coordinador de seguridad de la información.

o Ejecutar las pruebas que cumplan con las funciones requeridas para la operación adecuada en el datacenter principal, actividad a cargo de cada uno de los líderes de equipo de recuperación: Coordinador de infraestructura, Coordinador de base de datos, Coordinador de seguridad de la información.

o Verificación con el personal de tecnología el funcionamiento de la aplicación con cada uno de los líderes de los procesos.

o Ejecutar orden de retorno a normalidad, actividad a cargo del jefe de tecnología y comunicaciones, iniciando por los procesos más críticos.

o Validar el funcionamiento del sistema de información en los procesos críticos y la restauración de los procesos no críticos, según el nivel de prioridad identificada, actividad a cargo de coordinador de seguridad de la información con apoyo de: ingenieros de base de datos, Ingeniero de imágenes diagnósticas, jefe de enfermería de historia clínica.

o Elaboración de reporte de restablecimiento de servicio anexo G. “Reporte de restablecimiento de servicio”, el cual tendrá que ser firmado por el jefe de tecnología y comunicaciones.

o Seguimiento y coordinación con los colaboradores que hacen uso del sistema de información tecnológica y las integraciones correspondientes, actividad a cargo del coordinador de seguridad de la información.

o Elaboración del informe del incidente que causo la no disponibilidad, los efectos, y la eficacia del plan de recuperación, las lecciones aprendidas y las mejoras que se deben implementar en el plan, actividad a cargo del coordinador de seguridad.

8.6 ESTRATEGIA AFECTACIÓN PARCIAL DE SERVINTE – ESTRATEGIA RECUPERACIÓN TECNOLÓGICA POR ALTA DISPONIBILIDAD

Esta estrategia se tendrá que activar en el momento que falle alguno de los siguientes elementos tecnológicos del centro de datos, los cuales se deberán encontrar en el centro de datos de hospital Méderi o en su sede Barrios Unidos con un mismo dispositivo espejo (Alta disponibilidad):

- Firewall: Dispositivo configurado y dispuesto en rack con tecnología alta disponibilidad.

- Switch´s: Se tendrá dispositivo de interconexión switch pre configurado para restaurar proceso crítico en caso de falla.

- Router´s: Se tendrá dispositivo de interconexión Router pre configurado para restaurar proceso crítico en caso de falla.

- Servidor de base de datos (Tecnología RAID 1+0): Todos los servidores utilizados para Servinte deberán tener un snapshop, con el fin de restaurar los servicios en el menor tiempo posible.

- Canal de internet: Se tendrá alternativa de conexión a internet por medio de un canal de internet alternativo el cual deberá ser de un ISP diferente al principal.

No aplica para dispositivos o sistemas que requieran una comunicación activa entre las dos sedes o que los cuales sean el único medio de protección contra determinada vulnerabilidad:

- Equipamiento auxiliar
- Canal de comunicación
- Respaldo UPS

Se resalta que si se presenta una falla que afecte el activo principal y se cuente con un backup de cualquiera de los anteriores dispositivos como por ejemplo el canal de internet (en el caso del hospital Méderi cuenta con un canal secundario de backup), y se excede el RTO definido para los procesos críticos que se estén viendo afectados parcialmente, se debe activar el plan de recuperación de desastres como medida correctiva y con un plan de acción eficiente y eficaz.

- Fase 1: planeación y alistamiento de activos de información de repuesto

o Se recibe el reporte generando un ticket en mesa de ayuda. Los ingenieros de Base de datos realizan la evaluación del caso y si es de su competencia es asignado al personal responsable.

o Detallar cada uno de las fallas que conllevan a la generación del incidente, actividad liderada por el coordinador de infraestructura.

o Verificar si es una falla general o solo se presenta parcialmente, actividad liderada por el coordinador de infraestructura con apoyo de Analistas de data center y soporte técnico.

o El coordinador de infraestructura deberá reportar el incidente según plan de comunicaciones.

o Se activa el plan de recuperación por parte del Jefe de tecnología y comunicaciones o quien haga sus veces, por medio del formato Anexo F. “Reporte de incidente Servinte”

o Preparar la puesta en marcha del dispositivo configurado en alta disponibilidad, actividad a cargo del coordinador de infraestructura con apoyo de analistas de data center.
o Organización de reunión de inicio del plan de recuperación con el equipo de recuperación, Actividad a cargo del coordinador de Seguridad de información o quien haga sus veces.

- Identificar con el personal encargado de la recuperación, los dispositivos críticos para restablecimiento normal del servicio (dispositivos/ servicios en alta disponibilidad), según los roles y responsabilidades, actividad a cargo del Jefe de tecnología y comunicaciones o quien haga sus veces.

- Verificar los servicios de terceros si se encuentran con la disponibilidad necesaria para iniciar el proceso de recuperación, actividad a cargo del Coordinador de infraestructura o quien haga sus veces.

- Validar y coordinar las actividades que son desarrolladas por colaboradores y proveedores para el desarrollo del plan de recuperación, actividad a cargo del Coordinador de seguridad de la información o quien haga sus veces.

- Probar funcionalidad de dispositivos / servicios en alta disponibilidad con la finalidad que se garantice el cumplimiento con las necesidades de procesamiento y operación necesaria para la recuperación de los procesos críticos, Actividad a cargo del Coordinador de infraestructura con apoyo de auxiliares de data center o quien haga sus veces.

- Fase 2: Recuperación y Validación de procesos y aplicaciones

- Iniciar el proceso de traspaso de servicio al dispositivo de alta disponibilidad, actividad a cargo del coordinador de infraestructura con apoyo de analistas de data center.

- Validación del funcionamiento del dispositivo y servicios soportados, actividad liderada por coordinador de infraestructura y supervisada por el coordinador de seguridad de la información.

- Verificar el plan de restauración de los procesos críticos según la prioridad identificada, actividad a cargo del jefe de tecnología y comunicaciones con apoyo del coordinador de seguridad de la información.

- Brindar el soporte técnico requerido a los usuarios internos y colaboradores, actividad a cargo de los auxiliares de soporte.

- Seguimiento al desempeño de los recursos tecnológicos que soportan la recuperación de los procesos identificados como críticos, actividad a cargo del coordinador de seguridad de la información y coordinador de seguridad de la información.
- Seguimiento y coordinación con los colaboradores que hacen uso del sistema de información tecnológica y las integraciones correspondientes, actividad liderada por el jefe de tecnología y comunicaciones con apoyo del coordinador de seguridad de la información.

- Fase 3: Normalización y afinamiento de las operaciones.

o Dimensionar el daño ocasionado por el incidente, si se define que la falla puede llegar a exceder el RTO nivel alto (según BIA) o bien puede llegarse afectar otros activos críticos, se tendrá que retomar la estrategia “Estrategia afectación total de Servinte - Centro de datos alterno”. Actividad liderada por coordinador de seguridad de la información, con apoyo de coordinador de infraestructura, coordinador de base de datos, DBA.

o Valorar y verificar los dispositivos necesarios para restablecer las operaciones al servicio normal, actividad a cargo del coordinador de infraestructura.

o Definir en conjunto con el equipo de recuperación el tiempo indicado para restablecer a la normalidad las operaciones, actividad a cargo del jefe de tecnología y comunicaciones.

o Planear el momento de restablecer los dispositivos principales sin ocasionar afectación a los procesos críticos, actividad a cargo del jefe de tecnología y comunicaciones.

o Elaboración del informe del proceso de restauración a la normalidad de las operaciones con el dispositivo/servicio primario, actividad a cargo del coordinador de infraestructura con apoyo del coordinador de seguridad de la información.

o Coordinar las actividades de restauración de dispositivo/servicio principal, actividad a cargo del jefe de tecnología y comunicaciones con apoyo del equipo de recuperación.

o Ejecutar las pruebas que cumplan con las funciones requeridas para la operación adecuada del dispositivo/servicio principal, actividad a cargo de cada uno de los líderes de equipo de recuperación: Coordinador de infraestructura, Coordinador de base de datos, Coordinador de seguridad de la información

o Ejecutar la normalización del dispositivo/servicio principal, actividad únicamente autorizada por el jefe de tecnología y comunicaciones mediante firma en el formato anexo F. “Reporte de incidente de Servinte”, actividad a cargo del coordinador de infraestructura

o Validar si el proceso de restauración del dispositivo/servicio principal ha resultado óptimo, actividad a cargo del Coordinador de infraestructura, Coordinador de base de datos, coordinador de seguridad de la información.

o Validar el apropiado funcionamiento del sistema de información en los procesos críticos y la restauración de los procesos no críticos, según el nivel de prioridad

identificada, Actividad a cargo de Coordinador de seguridad de la información con apoyo de: Los ingenieros de base de datos, los ingenieros de imágenes diagnósticas, el jefe de enfermería y de historia clínica.

- Elaboración de reporte de restablecimiento de servicio anexo G. “Reporte de restablecimiento de servicio”, el cual tendrá que ser firmado por el Jefe de tecnología y comunicaciones y dirigido a los líderes de procesos críticos.

- Seguimiento y coordinación con los colaboradores que hacen uso del sistema de información tecnológica y las integraciones correspondientes, actividad a cargo del coordinador de seguridad de la información.

- Elaboración del informe del incidente que causo la no disponibilidad, los efectos, y la eficacia del plan de recuperación, las lecciones aprendidas y las mejoras que se deben implementar en el plan, actividad a cargo del equipo de recuperación, se debe diligenciar los campos correspondientes mediante el formato anexo F“ reporte de incidente Servinte”.

8.7 ESTRATEGIA PREVENTIVA PARA PERDIDA DE INFORMACIÓN (COPIAS DE RESPALDO)

Adicional a las estrategias descritas en los puntos anteriores, se define una estrategia de recuperación de información almacenada en la base de datos de Servinte, para este fin y teniendo en cuenta los RPO identificados se define el respaldo de información la cual se tendrá que realizar de la siguiente manera:

8.7.1 Copia de seguridad diaria

- 2 copias incrementales las cuales se realizarán a las 6:00 am y 2:00 pm
- 1 copia de seguridad nivel 0 la cual se iniciar a las 1:00 am

8.7.2 Copia de seguridad semanal

- 1 copia de seguridad semanal completa, la cual se realizará el día sábado a partir de la 11:00 pm

8.7.3 Copia de seguridad mensual

- 1 copia de seguridad mensual completa, la cual se realizará el último día de cada mes 2:00 am

8.7.4 Retención de backups. Teniendo en cuenta el volumen de la información y el uso limitado de espacio de almacenamiento, se tendrá que tener en cuenta condiciones de retención de backups:

- Únicamente se tendrán almacenados los backups diarios realizados en los últimos 5 días, dando en custodia a un tercero.

- Se mantendrán los backups semanales de las últimas 4 semanas, al final del mes se mantendrá únicamente el backup mensual las demás serán eliminadas.

- Se mantendrá 12 backup mensuales organizados por año por los últimos 3 años, dando en custodia a un tercero.

- Las actividades de copia de seguridad y traslado de cintas al custodio serán lideradas por el coordinador de infraestructura.

8.8 PROCEDIMIENTO DE ACTIVACIÓN DRP

8.8.1 Detección y registro del incidente. La detección de interrupción se dará por parte del personal operativo quien estará intrínsecamente ligado a cada uno de sus procesos y serán quienes vean la afectación de manera inmediata, esta detección se tendrá que dar por medio de un requerimiento a la mesa de ayuda quienes inicialmente determinaran la gravedad haciendo una evaluación inicial de la falla, documentando la solicitud implementada.

8.8.2 Evaluación de daños. La evaluación de daños se dará de acuerdo a la evaluación inicial de la mesa de servicio, quien asignará la solicitud al responsable según la naturaleza de la falla, la cual puede ser de infraestructura tecnológica, fallas en la base de datos, fallas en telecomunicaciones o un desastre masivo que involucre cada uno de los elementos del centro de datos.

Para la apropiada evaluación de los daños y posterior activación de DRP y aplicación de estrategia se deberá enfrentar a los siguientes interrogantes, los cuales evidenciaran si la falla es parcial o total.

- ¿Cuál fue la causa inicial de la interrupción?

- ¿Cuál falla es un problema conocido o ha sido reiterativo?

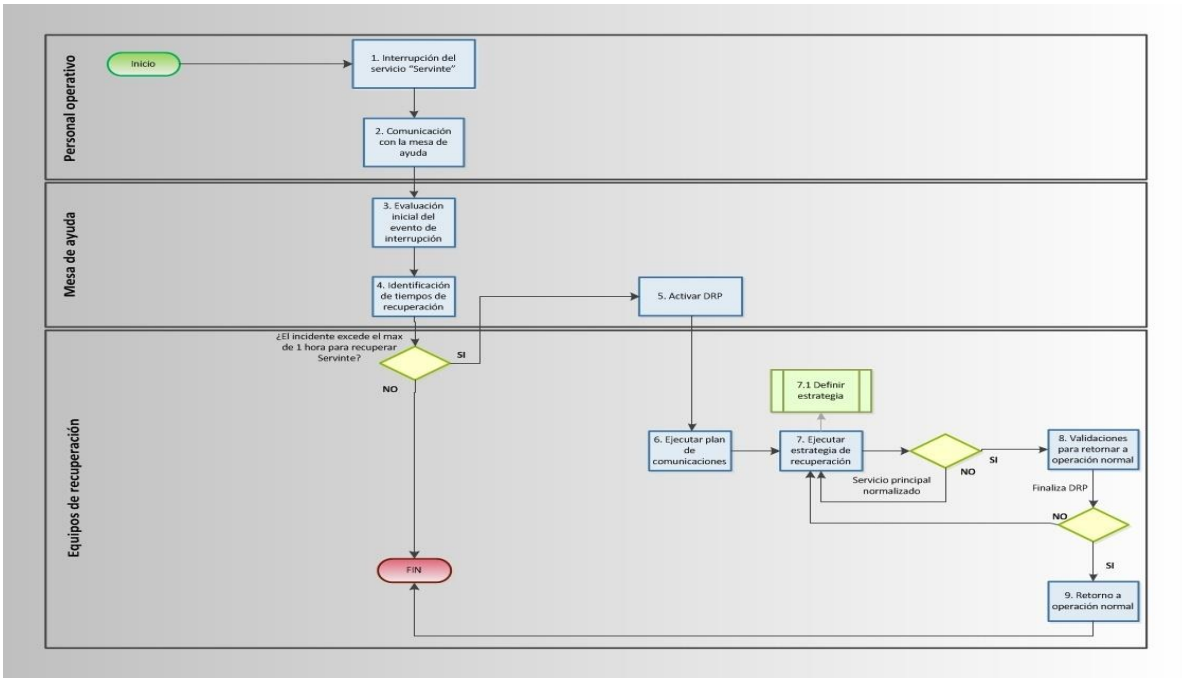
- ¿Cuál es el estado funcional de los equipos informáticos (totalmente funcional, en parte funcional y no funcional)?

- ¿Qué tipo de elementos son declarados no funcionales, estos pueden ser recuperados o sustituidos inmediatamente (máximo una hora)?

Si al evaluar estos interrogantes se llega a la conclusión de que el sistema Servinte y uno o más activos de información que lo soportan no pueden ser recuperados en máximo una hora (tolerancia máxima del proceso más crítico según definición de RTO), se tendrá que notificar al equipo de recuperación según corresponda en el plan de comunicaciones y de esta manera iniciar el manejo de la crisis, dando respuesta planificada al incidente según corresponda.

Mediante el procedimiento relacionado en la figura, se define los actores responsables y las actividades que se han de seguir para la activación del DRP y administración de la crisis: (Ver figura 5)

Figura 5. Procedimiento administración de crisis



Fuente: autores

Se relaciona el detalle de cada una de las actividades definidas en el procedimiento de administración de crisis. (Ver cuadro 38)

Cuadro 21. Detalle de procedimiento administración de crisis

Numero	Entrada	Actividad	Salida	Descripción	Responsable
1	Inicio	Interrupción del servicio Servinte	Establecer conexiones con soporte	El personal de hospital Méderi y sede en Barrios Unidos, quienes están se verán directamente afectados por la interrupción del servicio Servinte, serán los primeros en evidenciar una caída del sistema o indisponibilidad del servicio, por lo tanto tendrán que reportar del evento mediante un requerimiento a la mesa de ayuda en el sistema Almera.	Funcionarios Hospital Méderi y sede en Barrios Unidos
2	Establecer conexiones con soporte	Comunicación con mesa de ayuda	Conexiones establecidas con Mesa de ayuda	La mesa de ayuda tendrá que empezar a tratar el requerimiento siendo los responsables de comentar los hallazgos iniciales del evento.	Funcionarios Hospital Méderi y sede en Barrios Unidos
3	Requerimiento creado en Almera	Evaluación inicial del evento de interrupción	Diagnóstico del requerimiento	Los responsables de mesa de ayuda, avaluaran la criticidad del evento, según su naturaleza, con herramienta de decisión basada en el análisis de riesgos y BIA	Mesa de ayuda
4	Diagnóstico del requerimiento	Identificación de tiempos de recuperación	Tiempos identificados	Según el nivel de criticidad definidos, activos de información afectados, procesos críticos afectados, se deberá estimar un tiempo máximo para la recuperación del servicio Servinte, se deberá enfrentar a la siguiente decisión: ¿El incidente excede el max de 1 hora para recuperar Servinte? SI: Continúe a la actividad 5 NO: Mesa de ayuda tratara el evento y finaliza el procedimiento	Mesa de ayuda

Cuadro 38. (Continuación)

Numero	Entrada	Actividad	Salida	Descripción	Responsable
5	Tiempos identificados	Activar DRP	Incidente reportado en requerimiento	El líder de mesa de ayuda, será el responsable de activar el plan de recuperación de desastre. Inicialmente realizando el plan de comunicaciones, activando el equipo de recuperación y re categorizando el evento reportado como un incidente confirmado Finalmente se debe registrar la información completada hasta esta etapa, en el formato "Reporte de incidente"	Mesa de ayuda
6	Incidente reportado en requerimiento	Ejecutar plan de comunicaciones	Equipo de recuperación informado	Una vez declarada la crisis por el incidente de interrupción ocurrido, se debe citar al equipo de recuperación, informar a todos los involucrados según el plan de comunicaciones de la situación y establecer el ambiente apropiado para la toma de decisiones. Los miembros del equipo necesitaran entender el escenario de falla que ellos van a enfrentar, así como los planes de recuperación que serán activados.	Líder de equipo de recuperación
7	Equipo de recuperación informado	Ejecutar estrategia de recuperación	Incidente de seguridad tratado	Luego de definida la estrategia, se deberá ejecutar según la secuencia que se indique. Se deberá enfrentar al siguiente cuestionamiento: ¿Servicio principal normalizado? SI: Continuar a la actividad 8 NO: Continuar a la actividad 7	Equipo de recuperación
7.1	Ejecutar estrategia de recuperación	Definir estrategia a aplicar	Estrategia definida	Tomar las decisiones acerca de cómo se debe tratar el incidente de seguridad confirmado con la prioridad definida, de acuerdo a si de evalúa una inoperatividad parcial o total del sistema Servinte	Equipo de recuperación

Cuadro 38. (Continuación)

Numero	Entrada	Actividad	Salida	Descripción	Responsable
8	Incidente de seguridad tratado	Validaciones para retornar a operación normal	Validaciones positivas	Durante el desarrollo de estas actividades, el Equipo de recuperación deberá realizar una labor de monitoreo, seguimiento y supervisión constante de todas las actividades desarrolladas con el fin de prever desviaciones, anticiparse a posibles problemas adicionales y estar atentos a suministrar los recursos y tomar las decisiones que se requieren para el normal desempeño y recuperación del sistema Se debe enfrentar el siguiente cuestionamiento: ¿Finalizar el DRP? Si: Continuar a la actividad 9 No: Continuar a la actividad 7	Equipo de recuperación
9	Validaciones positivas	Retorno a operación normal	Monitoreo	Durante esta actividad se realizarán las actividades para el retorno a la operación normal del sistema de información Servinte. Estas actividades incluyen: Recuperación de los activos de información afectados.	Equipo de recuperación
9	Validaciones positivas	Retorno a operación normal	Monitoreo	Informar a todo el personal involucrado que la crisis ha sido superada. Oficializar el inicio de las operaciones con los activos de información principales. Durante este tiempo, el equipo de recuperación, tendrá que realizar monitoreo al desarrollo y resultado de estas actividades, para asegurar que se ejecuten de la manera correcta y los procesos críticos afectados normalicen su funcionalidad.	Equipo de recuperación
Fuente: autores					

8.9 PLAN DE COMUNICACIONES

8.9.1 Alcance. Mediante este plan de comunicaciones se establece el orden jerárquico y la manera mediante la cual se debe realizar el proceso de comunicación de un eventual incidente que requiera la activación del plan de recuperación de desastres, enfocado al equipo de recuperación definido que deberá tratar la inoperatividad del sistema Servinte y los procesos críticos identificados.

8.9.2 Objetivo

- Identificar personal crítico a ser comunicado en un eventual incidente de seguridad que afecte al sistema Servinte en uno o más de sus procesos críticos definidos

- Informar en el menor tiempo posible a cada uno de los integrantes del equipo de recuperación, con el fin de tomar plan de acción requerido para tratar eventuales incidentes que afecten el adecuado funcionamiento del sistema Servinte.

8.9.3 Equipo de recuperación. El equipo de recuperación estará dispuesto según apartado Estrategias de recuperación, cada uno de sus integrantes será responsable de realizar la comunicación de la crisis según la cascada de comunicación.

En el caso que un integrante del equipo de recuperación no se encuentre disponible se tendrá que suplir su cargo y por ende sus roles y responsabilidades por el cargo alterno. (Ver cuadro 34)

8.9.4 Principios para comunicación efectiva

- Información rápida y precisa: la información que se transmita en un mensaje o llamada deberá ser lo más inmediata posible y se le debe dar la prioridad y la importancia que el tema requiere.

- Claridad en la comunicación. Se debe procurar que no exista ambigüedad en la expresión de la idea, se deberá resumir lo mejor posible sin omitir información importante, la comunicación deberá ser calmada, honesta y centralizar la idea principal.

- Exactitud de la información: Se tendrá que transmitir la información relevante al contexto que se tenga en cuanto a la generación y tratamiento del incidente, no se

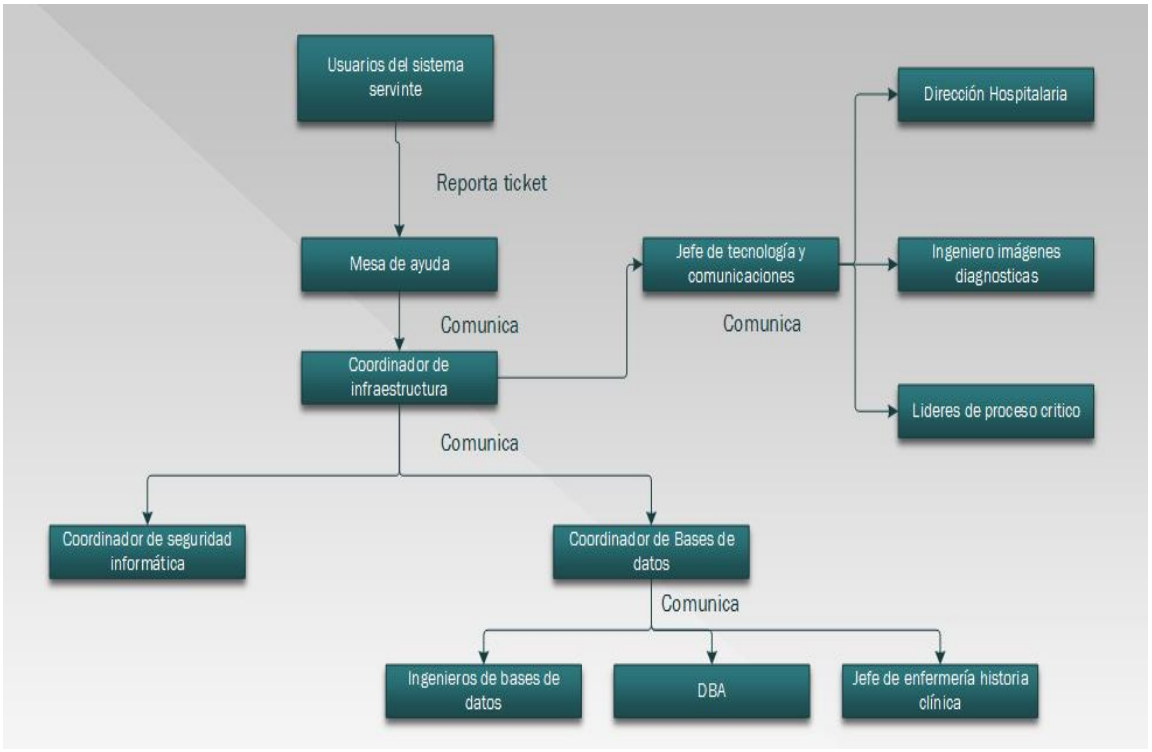
debe especular sobre alguna situación o emitir diagnósticos, opiniones o hipótesis sin tener certeza del argumento expresada

- Información constante: En caso que su interlocutor no se encuentre en hospital Méderi o su sede en Barrios Unidos, se tendrá que establecer información de manera constante, informando en todo momento el estado del incidente o tema tratado.

- Confidencialidad de la información: Es de vital importancia destacar la debida precaución que se debe tener al trasmitir mensajes o información de ámbito confidencial por medios telefónicos o transmisiones no seguras.

8.9.5 Cascada de Comunicación. En el momento de la presentación de un eventual incidente se deberá seguir la cascada de comunicación definida, dicha comunicación se tendrá que dar de manera inmediata a cada uno de los integrantes del equipo de recuperación: (Ver figura 6)

Figura 6. Cascada de comunicación



Fuente: autores

8.9.6 Contactos Equipo de recuperación. Se relacionan los datos de contacto de cada uno de los integrantes del equipo de recuperación. (Ver cuadro 39)

Cuadro 22. Contactos equipo de recuperación

Cargo	Nombre	Correo institucional	Correo personal	Celular	Extensión
Jefe de tecnología y comunicaciones					
Coordinador de infraestructura					
Coordinador de base de datos					
Coordinador de seguridad de la información					
Administrador base de datos					
Ingeniero de base de datos 1					
Ingeniero de base de datos 2					
Desarrollador					
Ingeniero de imágenes diagnosticas					
Jefe de enfermería de historia Clínica					
Auxiliar de soporte Clínico					
Auxiliar data Center					
Técnico de soporte 1					
Técnico de soporte 2					
Técnico de soporte 3					
Fuente: autores					

8.9.7 Contactos Proveedores. Se relacionan los datos de contacto de cada uno de los proveedores de activos de información críticos para el funcionamiento del sistema Servinte. (Ver cuadro 40)

Cuadro 23. Contactos proveedores.

Servicio	Empresa	Correo electrónico	Teléfono	Extension	Celular
Internet principal					
Internet secundario					
Base de datos					
Servinte					
Firewall					
Aire acondicionado					
Sistema de alimentacion ininterrumpida					
Circuito cerrado de television					
Control de acceso					
Fuente: autores					

9. PLAN DE CONCIENTIZACIÓN Y COMPETENCIA

Debe ser implementado un programa coordinado para asegurar que regularmente se lleva a cabo el proceso de promover la consciencia del IRBC en general, así como la evaluación y el mejoramiento de la competencia del personal clave relevante para la implementación exitosa.[40]

9.1 ALCANCE

Se tendrá que capacitar y sensibilizar a todo el personal involucrado en el proceso de plan de recuperación de desastre de Hospital Méderi y su sede en Barrios Unidos:

- Dirección hospitalaria
- Equipo de recuperación
- Observadores de pruebas
- Líderes de proceso
- Proveedores

9.2 OBJETIVOS

- Identificar debilidades a reforzar en cuanto a las capacidades y consciencia de cada uno de los participantes del plan de recuperación de desastres.

- Asegurar el apropiado entendimiento del plan de recuperación desastres y la apropiada ejecución de actividades por parte de los integrantes del plan de recuperación de desastres y cualquier persona que intervenga en el mismo.

- Afianzar competencias y capacidades de cada uno de los actores intervinientes de tal manera que sean aplicadas de la mejor manera en el momento de la ejecución del plan de recuperación desastres.

- Establecer métodos que garanticen la apropiada trasmisión del mensaje de una manera interactiva.

- Evaluar los resultados obtenidos y el conocimiento adquirido por parte de la audiencia objetivo.

[40] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de gestión de la continuidad de negocio. NTC-ISO 22301. Bogotá D.C.: El instituto, 2012. 22 p.

9.3 ROLES Y RESPONSABILIDADES

Se define las responsabilidades que tendrá cada uno de las personas que tendrán a cargo impartir el conocimiento.

9.3.1 Líder plan de concientización y capacitación. El jefe de tecnología y comunicaciones será el encargado de este rol y tendrá las siguientes responsabilidades:

- Autorización de métodos y estrategias de aprendizaje
- Revisión de estadísticas evaluación de capacitaciones y aptitudes del instructor
- Velar por la apropiada asistencia y compromiso del personal relacionado con el plan de recuperación de desastres
- Establecer directrices que permitan la aplicación correcta y de manera eficiente las capacitaciones y sensibilizaciones a impartir

9.3.2 Instructor. El encargado de este rol será el coordinador de seguridad de la información y tendrá las siguientes responsabilidades:

- Organización de planificación de métodos de aprendizaje a aplicar a la audiencia
- Identificar debilidades a reforzar por medio de capacitaciones
- Presentar propuestas de capacitación ante el líder del plan de concientización y capacitación
- Diseñar y preparar las temáticas y evaluaciones a aplicar a la audiencia objetivo
- Impartir capacitaciones de acuerdo al cronograma programado
- Aplicar las evaluaciones diseñadas al finalizar cada una de las capacitaciones
- Realizar estadísticas de aprendizaje obtenido por parte de la audiencia.
- Actualización de plan de concientización y competencia como también los formatos relacionados.

9.4 AUDIENCIA Y ENFOQUE

Todas las personas involucradas en el proceso de recuperación de desastres del Servinte, será el público objetivo y como responsabilidad principal tendrán que participar en todas las capacitaciones y actividades relacionadas con el plan de concientización y capacitación para las que sean requeridos.

- Dirección hospitalaria: Al personal de dirección hospitalaria se tendrá que enfocar en temas consecuentes de los eventuales incidentes en términos de producción y operatividad, presentación del plan de recuperación de desastres, importancia del apoyo estratégico

- Equipo de recuperación: Para el equipo de recuperación será necesario aplicar temas de capacitación y sensibilización en cuanto a controles relacionados con seguridad de la información aspectos técnicos, tecnológicos, vulnerabilidades, ataques que pudiesen llegar a afectar la disponibilidad del sistema Servinte, manejo apropiado de eventuales incidentes, entendimiento de actividades roles y responsabilidades contenidos en el plan de recuperación de desastres.

- Líderes de proceso: Al personal responsable del liderazgo de cada uno de los procesos críticos identificados en BIA, se tendrá que impartir capacitación y concientización en cuanto al manejo y reporte inmediato de los incidentes, detección apropiada de incidentes.

- Observadores de prueba: Teniendo en cuenta que este personal podrá tener o no conocimiento técnico en cuanto a incidentes, contención de incidentes y términos tecnológicos, se tendrá que capacitar en aspectos principales de ataques a la seguridad de la información, modo de operación principal de los procesos críticos identificados y conocimiento del plan de recuperación de desastres.

- Proveedores: La temática enfocada a este tipo de audiencia deberá ser relacionada con aspectos principales de manejo de incidentes que afecten componentes y servicios proveídos por terceros, tiempos óptimos de recuperación, vulnerabilidades y controles de seguridad de la información.

9.5 MÉTODOS DE CAPACITACIÓN Y CONCIENTIZACIÓN

- Capacitación presencial
- Capacitación Virtual Moodle
- Campañas de sensibilización y concientización
- Boletines informativos y comunicados (correo, fondos de pantalla, etc.)
- Ingeniería social

9.6 EVALUACIÓN

Cada una de las capacitaciones realizadas tendrá que ser evaluadas con el objetivo de medir el nivel de entendimiento de la audiencia, se define el formato anexo I. Evaluación de conocimiento, adquirido para tal fin.

También será necesario que la audiencia diligencié el formato anexo J. Evaluación al capacitador, con el objetivo de medir la idoneidad y competencia del capacitador para transmitir ideas de manera clara, el interés del tema por parte de la audiencia,

9.7 CRONOGRAMA

Se deberá planear un cronograma anualmente, mediante la cual se registre la cantidad de capacitaciones que se deben realizar, la temática a tratar, la audiencia objetivo y metodología que se utilizara.

Se deberá registra y presentar según el siguiente formato de cronograma: (Ver cuadro 41)

Cuadro 41. Cronograma de capacitación y concientización

Tema de capacitación	Método de entrega	Responsable	Audiencia objetivo	Hora y fecha inicio	Hora y fecha final	Duración
Fuente: autores						

10. PLAN DE PRUEBAS

10.1 GENERALIDADES

En dirección a las buenas prácticas relacionadas con la norma 22301, se establece el siguiente plan de pruebas el cual pretende identificar los tiempos de respuesta y efectividad de las estrategias propuestas en el plan de recuperación de desastres.

Debido al alto requerimiento de operación 24 horas 7 días de la semana, ninguna de las pruebas a realizar podrá ser invasiva, ni podrá haber indisponibilidad del sistema Servinte, todas las pruebas a realizar se tendrán que realizar fuera de un ambiente de producción, con réplica en la base de datos y en los aplicativos necesarios.

Se debe elegir un equipo de observadores definidos por la dirección de hospital Méderi y los cuales no deben pertenecer al equipo de recuperación, ellos imparcialmente darán cuenta de cada uno de las actividades ejecutadas por los integrantes del equipo de recuperación y el resultado de las mismas, dichas observaciones deberán ser incluidas en el Formato de pruebas DRP – Servinte, en el apartado “observaciones”.

Mediante el formato anexo H “Formato Prueba DRP - Servinte”, se tendrá que definir detalladamente el proceso de la prueba de acuerdo a los siguientes ítems:

- Definición de cronograma. El Jefe de tecnología y comunicaciones con apoyo del Coordinador de seguridad de la información, establecerán las actividades principales que se deberán controlar en las pruebas a realizar, las cuales deberán definir un responsable por actividad, hora y fecha de inicio / finalización para cada una de las actividades.

Se definen inicialmente las siguientes; si el jefe de tecnología y comunicaciones requiere adicionar algunas los podrá hacer en el campo cronograma:

- Reunión de inicio
- Recolección de información y planeamiento
- Identificación de roles y responsabilidades
- Inicio de la prueba
- Finalización de la prueba
- Reunión de finalización
- Informe de prueba

- Identificación de riesgo asociado (Escenario de indisponibilidad). Se debe identificar los eventos y escenarios que puedan causar indisponibilidad, describir los riesgos asociados que se identificaron mediante la etapa de análisis de riesgo.

- Componentes involucrados. Relacione cada uno de los componentes tecnológicos críticos involucrados en la prueba a realizar.

- Control de cambios. Para el inicio de la prueba puede ocurrir que se necesite hacer alguna configuración adicional a los componentes tecnológicos involucrados en la prueba, todo cambio y/o configuración aplicada debe ser registrada en el campo control de cambios, donde se define el componente objeto de cambios, la descripción detallada del cambio, la persona responsable del activo o componente que apruebe el cambio y el ejecutor.

- Equipo de recuperación. Se tendrán que definir los integrantes del equipo de recuperación que participaran en la prueba de recuperación de Servinte, los cuales deberán tener claro sus roles, responsabilidades y actividades a desarrollar según se define en el apartado estrategia, equipo de recuperación.

- Observadores. La dirección hospitalaria designara, observadores en cada prueba de recuperación los cuales garantizaran la imparcialidad en los resultados de cada una de las actividades y resultados de las pruebas aplicadas, mediante esta figura también se podrá establecer objetivamente las oportunidades de mejora, debilidades, fortalezas y amenazas, puesto que dichos observadores tendrán la capacidad de estar en un escenario propicia para evitar ambigüedades y supuestos en la ejecución de la prueba, por lo tanto resultados más precisos y enfocados a una eventual indisponibilidad real del servicio.

- Actividades a realizar. Mediante la reunión de inicio de la prueba se deberá establecer claramente cada una de las actividades que se llevarán a cabo para el desarrollo de la prueba, dichos registros deberán contener:

  - Descripción de la actividad
  - Responsable de ejecutar la actividad
  - Fecha y hora de inicio en que se ejecuta la actividad
  - Fecha y hora final de la actividad
  - Tiempo total utilizado para la aplicación de la actividad
  - Resultado obtenido, si fue exitosa o fallida, porque razón

- Anexos y evidencias. En cada una de las actividades que se pudiesen ejecutar, se podrá evidenciar o no por medio de una evidencia (fotos, imágenes, capturas de pantalla, registros, reportes), dichas evidencias deben ser relacionadas en el reporte y adjuntadas al mismo.

- Conclusiones. En la reunión de clausura o de finalización de la prueba, los integrantes del equipo de recuperación y observadores, podrán aportar sus conclusiones y observaciones del proceso de pruebas.

- Firmas. Cada uno de los integrantes y observadores participantes en la prueba debe revisar el contenido del reporte y firmar en conformidad.

Cada plan de pruebas tiene establecidos unos objetivos, alcance y frecuencias de aplicación diferentes, los cuales son definidos a continuación.

10.2 PRUEBA ESTRATEGIA- CENTRO DE DATOS ALTERNO

10.2.1 Alcance. Ejecutar pruebas de restauración de la base de datos Informix y puesta en marcha de aplicativo Servinte en centro de datos alternos, dichas pruebas no podrán realizarse en un ambiente de producción ni con desconexión real del sistema, esto debido a la necesidad de operación 24/7 que se debe tener en el hospital Méderi y su sede en HUBU.

10.2.2 Objetivos

- Determinar el nivel de la capacidad de la estrategia definida para respaldar una operación normal en los procesos críticos definidos mediante el BIA.

- Medir los tiempos necesarios que conllevan la recuperación del sistema Servinte, la base de datos Informix, y puesta en marcha toda la infraestructura requerida para la apropiad disponibilidad del sistema Servinte en caso de un desastre.

- Validar la efectividad en la ejecución de cada una de las actividades según los roles de cada uno de los miembros del equipo de recuperación y su desempeño en la prueba.

- Identificar acciones de mejora que se requiera para el apropiado afinamiento del plan de pruebas, que permita mejor respuesta ante una indisponibilidad del servicio.

10.2.3 Frecuencia. Las pruebas realizadas a la estrategia de centro de datos alterno, se tendrá que realizar por lo menos 2 veces al año, con una periodicidad semestral.

10.3 PRUEBA ESTRATEGIA – RECUPERACIÓN TECNOLÓGICA POR ALTA DISPONIBILIDAD

10.3.1 Alcance. Ejecutar pruebas de restauración y puesta en marcha de dispositivos dispuestos en alta disponibilidad, las pruebas no podrán ser realizadas afectando el dispositivo o servicio principal y deberán estar aisladas totalmente del ambiente de producción,

10.3.2 Objetivos

- Determinar el nivel de la capacidad de la estrategia definida para respaldar una operación normal en los procesos críticos definidos mediante el BIA.

- Medir los tiempos de restablecimiento de dispositivos / servicios, que se encuentran en alta disponibilidad.

- Revisar la secuencia de actividades, roles y responsabilidades en la estrategia de alta disponibilidad, identificando posibles inconsistencias y fallas.

- Identificar acciones de mejora que puedan surgir en la ejecución de la estrategia de alta disponibilidad.

10.3.3 Frecuencia. Las pruebas realizadas a la estrategia de alta disponibilidad, se tendrá que realizar por lo menos 3 veces al año, a cada uno de los dispositivos / servicios definidos.

10.4 PRUEBA ESTRATEGIA DE BACKUPS

10.4.1 Alcance. Pruebas de integridad y disponibilidad a las copias de seguridad realizadas según estrategia de backups, dichas pruebas serán aplicadas a la información relacionada con el sistema Servinte que se encuentre contenida en el servidor de archivos y cintas entregadas en custodia.

10.4.2 Objetivos

- Comprobar la funcionalidad en la ejecución de las copias de respaldo realizadas según estrategia para los backup’s

- Verificar el cumplimiento de la periodicidad de toma de losbackup’s definidos en la estrategia.

- Identificar posibles fallas que se pudiesen llegar a generar en la realización de backup´s guardados en el servidor de backup’s y en las cintas que se entregan en custodia para disposición final.

- Revisar el apropiado funcionamiento de los backup’s almacenados.

- Medición de tiempos de recuperación de información de copias de respaldo en servidor de backup´s y cintas almacenadas.

- Identificar acciones de mejora que permitan reestablecer información dispuesta en backups, a la mayor brevedad.

10.4.3 Frecuencia. Las pruebas realizadas a la estrategia de backup´s, se tendrá que realizar por lo menos tres veces al año, aplicadas a las copias de información que se encuentren en el servidor de backup y cintas que se encuentren en custodia.

10.5 ACTIVIDADES

10.5.1 Actividades preliminares

- Definición de las fechas y la programación de la prueba, actividad a cargo del Jefe de tecnología y comunicaciones.

- Definición de tiempos óptimos en cada una de las actividades definidas en la estrategia, actividad a cargo del jefe de tecnología y comunicaciones.

- Convocar reunión con equipo de recuperación para realizar planeamiento de la prueba donde se definirán, objetivos, alcance, resultados esperados.

- Información del planeamiento y aplicación de la prueba a la dirección del hospital Méderi y HUBU.

- Identificación de responsables y actividades a desarrollar según la estrategia definida.

- El diligenciamiento del Anexo H “Formato Prueba DRP - Servinte”, lo deberá realizar el coordinador de seguridad de la información quien debe estar transversalmente en cada una de las actividades de la prueba.

10.5.2 Actividades durante la Prueba

- Los integrantes del equipo de recuperación deben seguir los roles, responsabilidades y actividades a realizar según se encuentre definido en cada una de las estrategias a probar.

10.5.3 Actividades posteriores

- Informa sobre clausura de las pruebas ante dirección del hospital Méderi y sede HUBU

- Reunión de finalización de la prueba, junto con equipo de recuperación, observadores y dirección hospitalaria.

- Revisión del resultado de la prueba, enfrentando los tiempos RTO Y RPO definidos en BIA

- Identificación de acciones de mejora a la estrategia.

- Acuerdos y seguimientos a acciones de mejora y compromisos adquiridos.

11. MANTENIMIENTO Y MEJORA

Este documento será evaluado por lo menos una vez al año o cuando sea necesario, teniendo en cuenta los procesos de prueba, cambios en el sistema Servinte o alguno de los aplicativos o infraestructura que lo soporta y las auditorias donde surgen las mejoras a realizar.

12. CONCLUSIONES

Mediante el desarrollo de este proyecto se generó una guía en la cual la Corporación hospitalaria Juan Ciudad Mayor - Méderi y su sede de Barrios Unidos puede tomarlo como insumo para su implementación como plan de recuperación del sistema de información Servinte en el caso que se llegase a presentar una no disponibilidad en alguno de sus activos que comprometa el correcto funcionamiento de Servinte.

Al realizar la identificación y el análisis de los riesgos que se pueden afectar el funcionamiento de Servinte y el impacto funcional para el desarrollo de las actividades de los empleados y colaboradores, permitiendo evaluar algunos de los controles con los cuales se puede disminuir la probabilidad de ocurrencia y determinar el riesgo que la empresa puede asumir, determinando su tiempos de recuperación, el punto de recuperación y así reducir el impacto que se ocasionaría a sus recursos, en la prestación del servicio, y la afectación financieras e imagen corporativa.

Con las estrategias planteadas se dan las posibles opciones con las cuales el departamento de tecnología puede contemplar para su implementación ya que se tuvieron en cuenta todos sus componentes tecnológicos y el recurso humano que soporta dicho sistema de información, con un esquema de pruebas que permiten evaluar el funcionamiento de las diferentes estrategias y así asegurar que el plan de recuperación de desastres cumpla el objetivo de minimizar el impacto de la no disponibilidad del sistema de información Servinte y recuperar su funcionamiento en el menor tiempo posible.

Las entidades de salud en Colombia deben tomar la protección de sus sistemas informáticos y de todos los elementos que los soportan como una prioridad de alto nivel, pues una falla o desastre que involucre la infraestructura tecnológica que opera y almacena información sensible y confidencial de las personas como son sus historias clínicas, puede llegar a ser catastrófico si no se cuenta con planes de continuidad de negocio que permitan prever las amenazas y riesgos a los que se encuentran expuestos. En el hospital está iniciando un trabajo arduo en implementar y mejorar su sistema de gestión de seguridad de la información SGSI, con el estudio de madurez realizado se evidencia que se tiene una deficiencia en varios dominios de la seguridad de la información queda por implementar nuevos y mejora los controles existentes y así fortalecer su SGSI, su objetivo cercano no es ser certificados en las norma ISO/IEC 27000, pero si por manejar buenas prácticas, el hospital cuente con procesos basados en estándares internacionales es una manera de brindar confianza a empleados, proveedores, colaboradores y los usuarios o pacientes que la información generada durante la atención o que es administrada por los diferentes procesos se maneja de una manera responsable y segura.

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ. Ley 80 de 1989 Creación del Archivo General de la Nación. Bogotá: Diario Oficial, 1989, 5 p.

BSI GROUP. ISO 22301: Sistema de gestión de continuidad del negocio. Guía Técnica Colombiana GTC 176 [En línea], disponible en Internet en: https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Normas ISO 31000. Bogotá: ICONTEC, 2009. 42 p.

CXO2CSO.com. Sitio alterno y centro de procesamiento. [En línea], disponible en Interneten:http://www.cxo2cso.com/2015/02/sitioalterno-y-centro-de-procesamiento. html

CORTE CONSTITUCIONAL. Ley 23 De 1981, Ética Médica. Colombia: Diario Oficial, 1981, 36 p.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (DAFP). Guía para la administración del riesgo. Cuarta Edición. Bogotá, DAFP, septiembre de 2011,52p.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, Procedimientos e impulso de la Administración Electrónica, Metodología de Análisis y Gestión de Riesgos de los sistemas de información. Libro 1 – Método. Bogotá: Magerit: Edición digital. 42 p.

HERNÁNDEZ, Ignacio. La formulación de proyectos. En ciencias e ingenierías. 1 ed, Reimpresión 2015. Bogotá D.C.: Universidad Piloto de Colombia, 2012. 272 p. ISBN: 978-958-8537-33-7.

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN. Sistema de gestión de la continuidad de negocio. NTC-ISO 22301. Bogotá D.C.: El instituto, 2012. 22 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y NORMALIZACIÓN. Referencias documentales para fuentes de información electrónicas. NTC 4490. Bogotá D.C.: El instituto. 1998. 27p

_____. Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación. NTC 1486. Bogotá D.C.: El instituto. 2008. 41p

_____. Referencias bibliográficas. Contenido, forma y estructura. NTC 5613. Bogotá D.C.: El instituto. 2008. 33p

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y NORMALIZACIÓN. Referencias documentales para fuentes de información electrónicas. NTC 4490. Bogotá D.C.: El instituto. 1998. 27p

KIRVAN, P. Plan para la recuperación de desastres RD-T1, 2015 [en línea].Disponible en internet: http://searchdatacenter. techtarget. com/es/crónica/ De -la -A- a-la-Z-plan- para-la-recuperación-de-desastres-RD-TI

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas, Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, Madrid, octubre de 2012, 42p.

MÉDICOS GENERALES COLOMBIANOS. Normas relacionadas con la historia clínica y la fórmula médica. [En línea]. Disponible en Internet en: https://www. medicosgeneralescolombianos.com/index.php?option=com_content&view=article& id=77:normas-relacionadas-con-la-historia-clinica-y-la-formula-medica&catid=33 &Itemid=22

MINISTERIO DE PROTECCIÓN SOCIAL. Manual de acreditación en salud, ambulatorio y hospitalario. Colombia. Versión 03, Bogotá, Octubre de 2011, 84p,ISBN: 978-958-8717-33-3

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución Número 1995 de 1999establecen normas para el manejo de la Historia Clínica. Colombia; Minsalud, 1999, p. 8

_____. Resolución Número 839 de 2017 por la cual modifica la resolución 1995 de 1999 y dicta otras disposiciones.Colombia; Minsalud, 2017, p. 7

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Tecnología de la Información. Técnicas de Seguridad. Código de práctica para controles de seguridad de la información GTC-ISO/IEC 27002:2013, Colombia: Mintic, 2015, 107p.

MORALES SOTO, Nelson Raúl. Plan hospitalario para desastres. (2000). disponible en internet: http://www. Planeamiento hospitalario. info/ contenido/ referencia/ PlanHospParaDesastres.pdf

NORMA **TÉCNICA** COLOMBIANA. ISO 27000, Tecnología de la información - Técnicas de seguridad - Sistemas de administración de la seguridad de la información - Visión general y vocabulario. Colombia: ICONTEC, 2008,

PLAN DE RECUPERACIÓN DE DESASTRES. ¿Qué es un drp? [En línea], disponible en Internet en: https://www.inbest.me/comunidad/que-es-un-drp

PROMO ACRONIS. Acronis. Retrieved 10 2015, from Acronis: [Enlínea]. Disponible en Internet en http://promo.acronis.com/rs/acronis/images/DR_Index_ 2012_ShortVersion_US_ EN_120130

SÁNCHEZ, Natalia. Plan de recuperación de desastres DRP. (2013, marzo) disponible en DISASTER-RECOVERY. Recuperación desastres. http://blog. celingest.com/2013/03/01/ recuperación- desastres-disaster-recovery/

SGSI. Seguridad de la Sociedad: Sistemas de Continuidad de Negocio – Requisitos. Suiza: Internacional/IEC Estándar 22301:2012, 2012, 38 p.
SIGNIFICADOS. COM. ¿Qué es resiliencia? [En línea], disponible en Internet en: https://www. significados.com/resiliencia/

_____. ¿Qué es sistema de información? [En línea], disponible en Internet en: https://www.significados.com/sistema-de-informacion/

SLIDESHARE. Marco legal de la historia clínica y registros clínicos del cuidado. [En línea]. Disponible en internet en:https://es.slideshare.net/jfg7max/marco-legal-de-la-historia-clinica-y-registros-clinicos-del-cuidado

UNIVERSIDAD SANTIAGO DE CALI. Gestión de calidad, términos y definiciones. [En línea], disponible en Internet en: http://www.usc.edu.co/index.php/gestion-de-calidad/terminos-y-definiciones

VISIÓN SOFTWARE, Seguridad de la información: sabía que la más mínima pérdida de información dentro de su empresa puede tener consecuencias irremediables. (2016, agosto). [En línea]. Disponible en internet en: http://www.visionsoftware.com.co/sabia-que-la-mas-minima-perdida-de-informacion-dentro-de-su-empresa-puede-tener-consecuencias-irremediables/

ANEXOS

Anexo A. Cuestionario BIA para líderes de proceso

Cuestionario definido para la obtención de datos respecto al impacto, RTO y RPO de cada uno de los procesos identificados en el hospital Méderi y su sede en barrios unidos, este cuestionario será aplicado a los líderes de proceso.

Cuestionario BIA para líderes de proceso			
Nombre de proceso		Fecha	
Líder a cargo			
1.	Identificación de Impacto		
1.1	Afectación del Proceso		
	Pregunta		Nivel de impacto
Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso en caso que se tenga indisponibilidad del sistema Servinte			
1.2	Reputación		
	Pregunta		Nivel de impacto
Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso a nivel reputaciones teniendo en cuenta la opinión del cliente, proveedores, sector financiero, gubernamental y público en general.			
1.3	Financiero		
	Pregunta		Nivel de impacto
Teniendo en cuenta la tabla de Criterios para definición de impacto, evalué cuánto dinero dejaría de percibir el hospital en caso de indisponibilidad del sistema Servinte.			
1.4	Atención al paciente		
	Pregunta		Nivel de impacto
Evalué el tiempo máximo que puede tardar la recuperación del sistema Servinte para no causar traumatismo en la atención a los pacientes del hospital Mederi y su sede de Barrios Unidos			
Campo para ser diligenciado por el encargado de seguridad informatica			
Resultado de la calificación del proceso critico (∑ proceso nivel de impacto * ponderación porcentual)			
Si el proceso es calificado como critico, responda la 2 y 3 parte de este cuestionario			
2.	Definicion de Tiempo Objetivo de Recupeacion RTO		
	Pregunta	RTO	Justificación
2.1	Considere que ocurre un incidente de gran impacto que deja inoperante su área, de acuerdo a los criterio para definición de RTO; especifique el tiempo máximo que podría pasar cada uno de sus procesos antes de afectar considerablemente a la compañía (Tiempo Objetivo de Recuperación - RTO).		
3.	Definicion de Punto Objetivo de Recuperación RPO		
	Pregunta	Respuesta	
3.1	¿Existe para su proceso un procedimiento manual el cual se ejecuta en caso de falla del sistema Servinte?		
3.2	Diga cuánto tiempo puede trabajar su proceso de manera manual, sin que se vea afectado en gran medida el hospital Mederi y su sede en Barrios Unidos.		
_____ Nombre y firma del lider del proceso		_____ Nombre y firma del encargado de seg.informatica	

Anexo B. Cuestionario BIA tecnología

Cuestionario definido para la obtención de datos respecto a la infraestructura tecnológica, software y personal necesario para el adecuado funcionamiento y soporte del sistema Servinte, este cuestionario será aplicado al líder del proceso de tecnología y comunicaciones de hospital Méderi.

Cuestionario BIA Tecnologia			
Nombre de proceso		**Fecha**	
Cargo del lider			
	Pregunta		
4.1	Mencione los módulos del sistema Serviente que utiliza cada uno de los procesos del hospital Mederi y su sede de Barrios Unidos los cuales garanticen su adecuada operación.		
4.2	Identifique el software necesario para el funcionamiento de Servinte relacionado con cada uno de los procesos definidos a continuación		
4.3	Mencione cada uno de los servidores necesarios para el funcionamiento del sistema servinte relacinado a los procesos descritos a continuación		
Proceso		4.1	4.2	4.3
Pregunta		Respuesta		
4.4	Relacione el personal que soporta e interviene en el apropiado funcionamiento del sistema Servinte			
Pregunta				
4.5	Relacione a continuacion los elementos tecnologicos necesarios para el funcioanamiento del sistema Servinte			
Tipo	Descripción	Cantidad Sede mayor	Cantidad Barrios Unidos	
Nombre y firma del líder del proceso		**Nombre y firma del encargado de seg.informatica**		

Anexo C. Ejemplo de Cuestionario BIA para líderes de proceso, resuelto

Para la recolección de información en cuanto a impacto, RTO Y RPO de los procesos identificados en clínica Méderi y su sede Barrios Unidos, se aplicó el cuestionario definido en el anexo A, a continuación, se muestra un ejemplo del cuestionario resuelto por el líder de proceso de Urgencias.

Cuestionario BIA para líderes de proceso		
Nombre de proceso	Urgencias	Fecha
Lider a cargo	Jefe de urgencias	12/07/2017

1.	Identificación de Impacto	
1.1	Afectación del Proceso	
	Pregunta	Nivel de impacto
	Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso en caso que se tenga indisponibilidad del sistema Servinte	4
1.2	Reputación	
	Pregunta	Nivel de impacto
	Basándose en la tabla de Criterios para definición de impacto, diga qué nivel de impacto tendrá el proceso a nivel reputacional teniendo en cuenta la opinión del cliente, proveedores, sector financiero, gubernamental y publico en general	3
1.3	Financiero	
	Pregunta	Nivel de impacto
	Teniendo en cuenta la tabla de Criterios para definición de impacto, evalue cuánto dinero dejaría de percibir el hospital en caso de indisponibilidad del sistema Servinte.	4
1.4	Atención al paciente	
	Pregunta	Nivel de impacto
	Evalué el tiempo máximo que puede tardar la recuperación del sistema Servinte para no causar traumatismo en la atención a los pacientes del hospital Mederi y su sede de Barrios Unidos	4
	Campo para ser diligenciado por el encargado de seguridad informatica	
	Resultado de la calificación del proceso critico. O proceso nivel de impacto * ponderación porcentual)	3,85
	Si el proceso es calificado como critico, responda la 2 y 3 parte de este cuestionario	

2.	Definicion de Tiempo Objetivo de Recupeacion RTO		
	Pregunta	RTO	Justificación
2.1	Considere que ocurre un incidente de gran impacto que deja inoperante su área, de acuerdo a los criterio para definición de RTO; especifique el tiempo máximo que podría pasar cada uno de sus procesos antes de afectar considerablemente a la compañía (Tiempo Objetivo de Recuperación - RTO)=	1	Es el proceso por donde ingresan la mayoría de pacientes a la institución solicitando los servicios de salud con prioridad dependiendo de la clasificación de su estado de salud, realizando los registros en el modulo clínico es un servicio que debe estar en funcionamiento 7 x 24.

3.	Definicion de Punto Objetivo de Recuperación RPO	
	Pregunta	Respuesta
3.1	¿Existe para su proceso un procedimiento manual el cual se ejecuta en caso de falla del sistema Servinte?	La institución tiene un plan de contingencia manual el cual se activa por los jefes y coordinadores de cada una de las áreas, se realiza el ingreso de los pacientes con una aplicación de contingencia, se registran todos los datos necesarios para realizar la atención de los pacientes, las ordenes medicas, evoluciones medicas se realizan en los formatos pre impresos institucionales.
3.2	Diga cuánto tiempo puede trabajar su proceso de manera manual, sin que se vea afectado en gran medida el hospital Mederi y su sede en Barrios Unidos	8 Horas
	Nombre y firma del lider del proceso	Nombre y firma del encargado de seg.informatica

Anexo D. Cuestionario BIA tecnología, resuelto

Para la recolección de información en cuanto a la infraestructura tecnológica, software y personal necesario para el adecuado funcionamiento y soporte del sistema Servinte, se aplicó el cuestionario definido en el anexo B, a continuación, se muestra el cuestionario resuelto por el líder de tecnología y comunicaciones de hospital Méderi.

Cuestionario BIA Tecnologia			
Nombre del proceso	Tecnologia de la información	Fecha	
Cargo del lider	Jefe de TIC	14/07/2017	

	Pregunta
4.1	Mencione los módulos del sistema Serviente que utiliza cada uno de los procesos del hospital Méderi y su sede de Barrios Unidos los cuales garanticen su adecuada operación.
4.2	Identifique el software necesario para el funcionamiento de Servinte relacionado con cada uno de los procesos definidos a continuación
4.3	Mencione cada uno de los servidores necesarios para el funcionamiento del sistema servinte relacionado a los procesos descritos a continuación

Proceso	4.1	4.2	4.3
Urgencias	Tablero hospitalizacion(Historia Clinica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermeria)	SERVINTE,Visor PDF, Agility, Mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión Internet, Servidor de PDF.
Clinicas Medicas	Tablero hospitalizacion(Historia Clinica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermeria)	SERVINTE,Visor PDF, Agility, Mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión,Servidor de PDF.
Salud sexual y reproductiva	Tablero hospitalizacion(Historia Clinica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermeria)	SERVINTE,Visor PDF, Agility, Mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión Internet,Servidor de PDF.
Cuidado critico	Tablero hospitalizacion(Historia Clinica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermeria)	SERVINTE,Visor PDF, Agility, Mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión Internet,Servidor de PDF.
Programas especiales	Tablero hospitalizacion(Historia Clinica, Evoluciones Medicas, Ordenes Medicas, Historia de Enfermeria)	SERVINTE,Visor PDF, Agility, Mipres	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión Internet,Servidor de PDF.
Nutrición	Tablero hospitalizacion(Historia Clinica, Evoluciones Medicas, ordenes medicas)	SERVINTE, Visor de PDF	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresión Internet,Servidor de PDF.
Servicio farmacéutico	Tablero hospitalizacion(ordenes medicas), Suministros	SERVINTE, Visor de PDF	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Impresion, Servidor de Reportes.
Admisiones y autorizaciones	Tablero de Admisiones, Autorizaciones, Consulta de Tablero hospitalizacion.	SERVINTE, Visor de PDF	Servidor de Aplicaciones, Servidor de Reportes,Servidor de Impresion, Impresoras.
Imágenes diagnosticas	Tablero hospitalizacion(Historia Clinica, Evoluciones Medicas, Ordenes Medicas)	SERVINTE, Visor de PDF,Agility	Servidor de Aplicaciones, Servidor de Integraciones de Imagenes Diagnositcas
Laboratorio clinico y servicio transfucional	Tablero hospitalizacion(Historia Clinica, Ordenes Medicas), Facturacion.	SERVINTE, Visor de PDF	Servidor de Aplicaciones, Servidor de Integraciones Laboratorio
Referencia y contrareferencia	Tablero hospitalizacion(ordenes Medicas)	SERVINTE, Visor de PDF	Servidor de Aplicaciones
Enfermeria	Tablero hospitalizacion(Historia Clinica, Ordenes Medicas, Historia de Enfermeria)	SERVINTE, Visor de PDF,Agility	Servidor de Aplicaciones, Servidor de Componentes, Servidor de Integraciones Imagenes y Laboratorio,Servidor de PDF.
Facturación	Facturacion(Analisis de Cuentas), Reportes	SERVINTE, Visor de PDF.	Servidor de Aplicaciones, Servidor de Componentes, servidor de impresion, Servidor de Reportes,Servidor de PDF.
Logística y suministro	Suministros, Cuentas por pagar,Maestros de suministros	SERVINTE, Docuclass	Servidor de Aplicaciones, Servidor de reportes, Servidor de impresión.
Inteligencia de negocios	N/A	Qlik View,SERVINTE	conexion a Base de datos
Tecnologia de la información y comunicaciones	Tablero Hospitalizacion, Tablero Consulta Externa, cartera, contabilidad, Cuentas por pagar, Facturacion, caja y Bancos,Suministros,	PUTY,SERVINTE, Visor de PDF,RAZOR SQL, Agility	base de datos, Servidores de Aplicaciones, Servidores de componentes, Servidor de Reportes, Servidor de Impresion
Cartera	Cartera	SERVINTE, Visor de PDF	Servidores de Aplicaciones, Servidor de reportes.

Tesoreria	Caja y Bancos	SERVINTE, Visor de PDF	Servidor de Aplicaciones, Servidor de Repores
Atención al usuario	N/A	Welcome, Almera	Conexion Base de datos
Auditoría medica	Tablero de hospitalizacion(Historia Clinica, Historia de Enfermeria, Ordenes medicas)	SERVINTE, Visor de PDF, Mipres	Servidor de Aplicaciones,Servidor de reportes

Pregunta		Respuesta
4.4	Relacione el personal que soporta e interviene en el apropiado funcionamiento del sistema Servinte	Jefe de Tecnologia y Comunicaciones (1) Coordinador de Infraestructura (1) Coordinador de Base de datos (1) Coordinador de Seguridad de la Informacion (1) DBA (1) Ingenieros de Base de datos (4) Desarrollador (1) Ingeniero de Imágenes Diagnosticas (1) Jefe de enfermeria de historia Clinica (1) Auxiliares de soporte Clinico (4) Auxiliar data Center (1) Tecnicos de soporte (6)

Pregunta

4.5 Relacione a continuacion los elementos tecnologicos necesarios para el funcioanamiento del sistema Servinte

Tipo	Descripción	Cantidad Sede mayor	Cantidad Barrios Unidos
Base de datos	Informix(BASE DE DATOS ORACLE)	1	Replica
Redes y comunicaciones	Routers	4	3
Redes y comunicaciones	swicth	40	16
Redes y comunicaciones	Firewall	2	1
Redes y comunicaciones	Canal de comunicaciones	etb y claro	une
Redes y comunicaciones	internet	etb y claro	une
Redes y comunicaciones	canal MPLS 16 servinte y 30 mbps imagenes	etb y claro	etb y claro
Redes y comunicaciones	Cableado estructurado	2500	500
Equip. Auxiliar	Aire acondicionado	3	1
Equip. Auxiliar	UPS Smart UPS RT 6000 VA 50kvas,30,29,10,6	8	3
Equip. Auxiliar	control de acceso	1	1
Equip. Auxiliar	deteccion y extincion de incendio	1	1
Equip. Auxiliar	control de temperatura y humedad	1	1
Equip. Auxiliar	cctv	1	1

Constanza Rodriguez Nombre y firma del líder del proceso	Sandra P Jara R Nombre y firma del encargado de seg.informatica

AnexoE. Análisis de Madurez

Se realiza un análisis de madurez y así dimensionar el grado de conformidad que se tiene en el hospital Méderi y su sede con respecto al estándar ISO/IEC 27001:2013, ya que se está en el camino de implementación y mejoramiento en los 7 dominios.

La evaluación se realizó con la siguiente tabla de valores la conformidad que se tiene con cada uno de los 114 controles del estándar ISO/IEC 27002:2013.

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	0
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	60
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	43
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	9
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	0
L5	100%	Optimizado	Los procesos están bajo constante mejora. Con base en criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	2
L6	N/A	No aplica		0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
A.5	**POLÍTICAS DE SEGURIDAD**	**Comprobar la existencia de una política de seguridad que cumpla con las exigencias definidas en el estándar ISO 27002. Así como que se encuentre aprobada por la dirección y las revisiones correspondientes.**		**100%**
A.5.1	**Directrices para la gestión de la seguridad de la información**			**100%**
A.5.1.1	Conjunto de políticas para la seguridad de la información	Se deben establecer formalmente las directrices que se deben seguir en Méderi para lograr los objetivos de seguridad de la información. En este sentido es necesario dar a conocer la política de seguridad de la información para informar y concientizar a todos los colaboradores y partes interesadas sobre los requisitos y criterios de protección establecidos para el “SGSI”.	L5	100%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
A.5.1.2	Revisión de las políticas para la seguridad de la información	Es necesario realizar una revisión periódica de las políticas de seguridad para garantizar la mejora continua; implementando las acciones y puntos de mejora para que las políticas se ajusten a los cambios de Méderi.	L5	100%
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Comprobar que está establecida una estructura de gestión para iniciar y controlar la seguridad de la información que cumpla con los puntos de control de este capítulo de la ISO 27002.**		**26%**
A.6.1	**Organización interna**			42%
A.6.1.1	Roles y Responsabilidades para la seguridad de la información.	Es necesario que los colaboradores de Méderi conozcan sus roles y responsabilidades relacionadas con la seguridad de la información para la correcta operación del SGSI, por tanto es importante que los miembros del Comité Directivo respalden activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de Méderi.	L3	90%
A.6.1.2	Segregación de funciones.	Se deben separar claramente los deberes para los roles establecidos, con el fin de que no se presenten conflictos de responsabilidades entre las áreas de Méderi que tienen acceso a los activos de información para que realicen un uso debido de los mismos.	L3	90%
A.6.1.3	Contacto con las autoridades	Es necesario que Méderi esté en contacto con las autoridades relacionadas con temas de seguridad de la información para mantenerse al día con las medidas de que debe implementar, contar con apoyo experto además de realizar una gestión oportuna a los incidentes de seguridad de la información en caso de presentarse.	L1	10%
A.6.1.4	Contacto con grupos de interés especial	Es necesario establecer contacto con grupos de interés especial en seguridad de la información como: foros o asociaciones profesionales para la atención de problemas que se puedan presentar en Méderi como fraudes, alertas, amenazas, vulnerabilidades, fallas de sistemas, problemas en productos de comunicación y desarrollo entre muchas otras falencias.	L1	10%
A.6.1.5	Seguridad de la información en la gestión de proyectos	Dada la importancia y sensibilidad de la información utilizada en los proyectos que se desarrollan dentro de las diferentes áreas dentro de Méderi, es necesaria la implementación de controles para ello.	L1	10%
A.6.2	**Dispositivos móviles y teletrabajo.**			10%
A.6.2.1	Política de uso de dispositivos móviles.	Los funcionarios mantienen información de la entidad en dispositivos móviles que debe ser manejada de acuerdo a los lineamientos del SGSI.	L1	10%
A.6.2.2	Teletrabajo.	Los funcionarios de Méderi pueden tener acceso remoto a los sistemas de información de Méderi para cumplir con sus labores. Además existe una normativa La Ley 1221 de 2008 “por la cual se establecen normas para promover y regular el teletrabajo y se dictan	L1	10%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
A.6.2.2	Teletrabajo.	otras disposiciones". Donde se establece que el TELETRABAJO es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.	L1	10%
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**	**Comprobar la seguridad ligada al personal observando la definición del trabajo y los recursos, la formación a los usuarios y la gestión de las incidencias y malos funcionamientos de seguridad.**		**39%**
A.7.1	**Antes de la Contratación**			70%
A.7.1.1	Investigación de antecedentes.	Debe hacerse una revisión de antecedentes y de aspectos de seguridad previo a la contratación del personal con el fin de mantener el riesgo operativo dentro de niveles aceptables. Para el desarrollo de las actividades de Consultoría, pruebas u otros contratos, la organización requiere contratar personal, los cuales tienen acceso a la información de la organización, por tanto es importante implementar controles basándose en los reglamentos, la ética y las leyes pertinentes, que aseguren un proceso de verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales previo acceso a la información.	L2	50%
A.7.1.2	Términos y condiciones de contratación.	Es necesario que en los contratos de funcionarios y contratistas se establezcan claramente las responsabilidades en cuanto a la seguridad de la información.	L3	90%
A.7.2	**Durante la contratación.**			37%
A.7.2.1	Responsabilidades por la dirección.	Es necesario que la presidencia de Méderi lidere y se comprometa con la implementación del SGSI y así asegurar el establecimiento de las políticas y los objetivos de seguridad de la información; para que estos estén alineados con el plan estratégico de Méderi PEM.	L2	50%
A.7.2.2	Toma de conciencia, capacitación y formación en la seguridad de la información.	Se debe sensibilizar al personal de Méderi para que tomen conciencia respecto a los riesgos de seguridad de la información.	L1	10%
A.7.2.3	Proceso disciplinario.	Se debe establecer un proceso disciplinario formal para las posibles faltas que puedan cometer las personas vinculadas o que hayan estado vinculadas con la institución respecto a la seguridad de la información para saber cómo proceder en dichos casos	L2	50%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.7.3	**Terminación o traslado de puesto de trabajo.**			10%
A.7.3.1	Terminación o cambio de puesto de trabajo.	Los colaboradores de la institución deben conocer sus deberes y responsabilidades relacionados con la seguridad de la información, durante su vinculación y cuando esta haya finalizado. Además cada vez que se le asignen nuevas responsabilidades o surja un cambio en ellas debe conocer los deberes relacionados con ellas.	L1	10%
A.8	**GESTIÓN DE ACTIVOS.**	**Observar si se mantiene una protección adecuada sobre los activos de la Organización y asegurar un nivel de protección adecuado a los activos de información.**		**44%**
A.8.1	**Responsabilidad sobre los activos.**			60%
A.8.1.1	Inventario de activos.	Es necesario establecer los activos de información y los activos relacionados con la información que están involucrados en los procesos de tratamiento de información de la entidad, con el fin de definir las responsabilidades de protección adecuadas.	L3	90%
A.8.1.2	Propiedad de los activos.	Es necesario establecer los responsables para cada activo y responsabilizarlos de: gestionar los riesgos de la información asociados a los activos a su cargo, cumplir los controles establecidos sobre el activo y establecer los custodios sobre estos activos.	L2	50%
A.8.1.3	Uso aceptable de los activos.	Se deben establecer las reglas de utilización para los activos de información. Los empleados, contratistas, aprendices, practicantes y los usuarios externos en general que usan o que tengan acceso a los activos de la organización deben tomar conciencia del uso. Se deben establecer las reglas de utilización para los activos de información. Los empleados, contratistas, aprendices, practicantes y los usuarios externos en general que usan o que tengan acceso a los activos de la organización deben tomar conciencia del uso.	L2	50%
A.8.1.4	Devolución de activos.	Se debe establecer un procedimiento que permita asegurar la devolución de los equipos y activos de información al momento de finalizar la relación laborar con funcionarios o contratistas.	L2	50%
A.8.2	**Clasificación de la información.**			23%
A.8.2.1	Directrices de clasificación.	De acuerdo a la importancia de la información manejada en los procesos misionales de Méderi, es necesario clasificar la información de la entidad basados en requisitos legales, valor, criticidad y susceptibilidad a divulgación modificación o acceso no autorizado.	L2	50%
A.8.2.2	Etiquetado y manipulado de la información.	Para asegurar que los activos de información de la institución reciben el nivel de protección adecuado, estos se deben clasificar teniendo en cuenta la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos.	L1	10%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.8.2.3	Manejo de activos.	Se deben implementar procedimientos que salvaguarden los requerimientos de clasificación y etiquetado definidos para los activos de información en la entidad.	L1	10%
A.8.3	**Manejo de los medios de almacenamiento.**			50%
A.8.3.1	Gestión de medios removibles o extraíbles.	La entidad maneja información de carácter confidencial en medios removibles que deben ser gestionados adecuadamente con el fin de asegurar que reciben el nivel de protección adecuado de acuerdo a las necesidades de Méderi.	L2	50%
A.8.3.2	Disposición o Eliminación de los medios.	Existe información sensible dentro de la prestación del servicio misional, que debe ser dispuesta de manera segura en caso de darla de baja de medios tecnológicos, del rehusó de equipos o del cambio de área de funcionarios.	L2	50%
A.8.3.3	Transferencia de los medios físicos	Los funcionarios y contratistas de la entidad utilizan medios físicos en tránsito que contienen información de la entidad por esta razón debe dárseles los niveles de seguridad adecuados para protegerlos contra accesos no autorizados, uso inadecuado o corrupción durante el transporte.	L2	50%
A.9	**CONTROL DE ACCESOS.**	**Comprobar si existen controles de acceso a la información como uso de contraseñas, privilegios, control del acceso remoto.**		**26%**
A.9.1	**Requisitos de negocio para el control de accesos.**			10%
A.9.1.1	Política de control de accesos.	La organización cuenta con activos de información que son manejados por los colaboradores, en tal sentido es importante establecer controles de seguridad que permitan asegurar que los propietarios de activos de información controlan el acceso a la información y a las instalaciones done esta es procesada, para esto se debe establecer, documentar y revisar una política de control de acceso basados en los requisitos de negocio y de seguridad de la información.	L1	10%
A.9.1.2	Control de acceso a las redes y servicios asociados.	Este control es indispensable para mantener los riesgos derivados por acceso no autorizado, manipulación de la información o difusión de malware, dentro de los niveles aceptables. La organización para su operación cuenta con una red LAN la cual soporta las actividades de los diferentes usuarios, por lo tanto es necesario establecer controles de seguridad para asegurar que los usuarios solo tienen acceso a los servicios para los cuales están autorizados.	L1	10%
A.9.2	**Gestión de acceso de usuario.**			10%
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	El personal de la entidad maneja diferentes tipos de información de acuerdo al área en la cual trabaja, por esta razón es muy importante tener un procedimiento que permita gestionar de forma adecuada el acceso de los usuarios a los sistemas y servicios de la institución.	L1	10%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	Debe existir un procedimiento formal de asignación de acceso de usuario que permita identificar el registro y cancelación de los usuarios o revocación de accesos para los diferentes sistemas y servicios de la entidad.	L1	10%
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	La asignación y uso de derechos de acceso con privilegios especiales debe ser restringido y controlado.	L1	10%
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	Debe existir un proceso de gestión formal para controlar la asignación de información de autenticación secreta de usuarios.	L1	10%
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	Para asegurar que los usuarios cuentan con los derechos de acceso apropiados, los propietarios de los activos deben revisar estos derechos de acceso a intervalos regulares.	L1	10%
A.9.2.6	Retirada o adaptación de los derechos de acceso	Se debe implementar un procedimiento para retirar los derechos de acceso a la información y a las instalaciones de procesamiento de la información de la institución, para todos los empleados y usuarios externos, al término de su relación laboral, contrato, o acuerdo, o bien cuando se realice un cambio en las labores que deben desarrollar.	L1	10%
A.9.3	**Responsabilidades del usuario.**			50%
A.9.3.1	Uso de información confidencial para la autenticación.	La información de autenticación a los diferentes sistemas debe mantenerse en secreto, por ello se debe exigir a los colaboradores el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.	L2	50%
A.9.4	**Control de acceso a sistemas y aplicaciones.**			34%
A.9.4.1	Restricción del acceso a la información.	Para evitar el acceso no autorizado a los sistemas y aplicaciones de la institución se debe restringir dicho acceso de acuerdo a la política de control de acceso de Méderi.	L2	50%
A.9.4.2	Procedimientos seguros de inicio de sesión.	El acceso a los sistemas y aplicaciones de la institución, debe ser controlado mediante un procedimiento de inicio de sesión seguro.	L2	50%
A.9.4.3	Gestión de contraseñas de usuario.	Debe implementarse un sistema para la gestión de contraseñas que sea interactivo y asegure que las contraseñas cumplan con los criterios de contraseñas fuertes establecidas en la entidad.	L2	50%
A.9.4.4	Uso de herramientas de administración de sistemas.	Para evitar la anulación de los sistemas o controles de las aplicaciones de la institución, se debe restringir y controlar el uso de los programas utilitarios que tengan la capacidad de sobrepasar los controles del sistema y de la aplicación.	L1	10%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.9.4.5	Control de acceso al código fuente de los programas.	El acceso al código fuente del programa e ítems asociados (como diseños, especificaciones, casos de uso y los planes de validación) deben ser estrictamente controlados, con el fin de evitar la introducción de funcionalidades no autorizadas y para evitar cambios no intencionales, así como para mantener la confidencialidad de propiedad intelectual valiosa.	L1	10%
A.10	**CIFRADO.**	**Se comprobará la gestión de la información cifrada en las operaciones.**		**10%**
A.10.1	**Controles criptográficos.**			10%
A.10.1.1	Política de uso de los controles criptográficos.	Se debe desarrollar una política en la institución, donde se establezca el uso de controles criptográficos, como cifrado de contraseñas y uso de llaves criptográficas ya que es indispensable para proteger la confidencialidad, la autenticidad y la integridad de la información.	L1	10%
A.10.1.2	Gestión de claves.	Méderi debe manejar mecanismos criptográficos para ciertos activos de información lo cual hace necesario la gestión de su gestión de llaves por medio de una política.	L1	10%
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL.**	**Se deben comprobar el cumplimiento de los puntos de control sobre seguridad física comprobando que existen áreas seguras, seguridad en los equipos y controles generales.**		**46%**
A.11.1	**Áreas seguras.**			37%
A.11.1.1	Perímetro de seguridad física.	Para prevenir el acceso no autorizado a áreas que contengan información confidencial o critica o a instalaciones de manejo de información se deben establecer perímetros de seguridad dentro de las instalaciones de la institución.	L1	10%
A.11.1.2	Controles de acceso físicos.	Se deben establecer controles de seguridad física para asegurar el acceso únicamente del personal autorizado a las áreas para las cuales se estableció un perímetro de seguridad.	L2	50%
A.11.1.3	Seguridad de oficinas, despachos e instalaciones.	Deben establecerse los controles de seguridad necesarios para evitar el acceso físico no autorizado y el daño a las oficinas e instalaciones de las sedes hospitalarias.	L2	50%
A.11.1.4	Protección contra las amenazas externas y ambientales.	La institución debe contar con protección contra daños causados por desastre natural (inundación, terremoto, tsunami, tormenta eléctrica, etc.), daños causados por ataque malicioso (explosión, revuelta civil, etc.), accidentes u otras formas de desastres por causa humana.	L2	50%
A.11.1.5	El trabajo en áreas seguras.	Méderi debe diseñar y aplicar procedimientos para trabajar en áreas seguras.	L1	10%
A.11.1.6	Áreas de acceso público, carga y descarga.	Deben implementarse controles para el área de despacho y carga, que por su criticidad y contando que el edificio tiene solo una entrada para este ingreso y salida, deben adecuarse los protocolos para garantizar la seguridad de la información en este caso los cuadernillos que van a la lectora.	L2	50%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.11.2	**Seguridad de los equipos.**			54%
A.11.2.1	Emplazamiento y protección de equipos.	La organización utiliza equipos tales como servidores, computadores de escritorio, portátiles, impresoras, fotocopiadoras, faxes, escáneres, entre otros, en estos equipos se procesa la información de los diferentes proyectos y de los procesos misionales de la institución por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo, interrupción de los equipos o compromiso de los activos de información.	L1	10%
A.11.2.2	Servicios de suministro.	El equipamiento institucional debe estar protegido contra fallas en el suministro de energía y otras interrupciones causadas por fallas en los elementos de soporte para prevenir la interrupción de las operaciones de la organización.	L3	90%
A.11.2.3	Seguridad del cableado.	Es necesario impartir instrucciones para proteger contra interceptación, interferencia o daños el cableado usado para energía y telecomunicaciones de la institución	L2	50%
A.11.2.4	Mantenimiento de los equipos.	Es necesario impartir instrucciones para asegurar que se haga el correcto mantenimiento de los equipos de cómputo de la institución.	L3	90%
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	Se debe implementar un procedimiento que establezca que se debe contar con una autorización formal previa al retiro de los equipos de cómputo, software o cualquier activo de información relevante para Méderi.	L2	50%
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Es necesario aplicar medidas de seguridad a los equipos y activos fuera de las instalaciones de la organización para protegerlos.	L2	50%
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	Se deben verificar todos los equipos de Méderi para revisar si contiene o no medios de almacenamiento antes de su eliminación o reutilización. Los medios de almacenamiento que contienen información sensible o con derecho de autor se deberían destruir físicamente o bien, la información se deberían destruir, eliminar o sobrescribir mediante técnicas para hacer que la información original no se pueda recuperar en vez de utilizar la función de eliminación o formateo normal.	L2	50%
A.11.2.8	Equipo informático de usuario desatendido.	Es necesario generar conciencia en los usuarios acerca de los requisitos de seguridad y los procedimientos para proteger los equipos desatendidos, como por ejemplo la buena práctica de bloquear la sesión para mantener segura la información almacenada en estos equipos.	L2	50%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	Para mejorar la seguridad de los activos es necesario implementar una política de escritorio limpio para papeles y medios de almacenaje removibles; y otra política de "pantalla limpia" para las instalaciones donde se procese información en la institución.	L2	50%
A.12	**SEGURIDAD EN LA OPERATIVA.**	**Se comprobara la gestión de las operaciones.**		**35%**
A.12.1	**Responsabilidades y procedimientos de operación.**			20%
A.12.1.1	Documentación de procedimientos de operación.	Se deben preparar procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación de información, como procedimientos de inicio y cierre de sesión de computadores, respaldo, mantenimiento de equipos, manejo de medios, salas de computación y administración y seguridad de manejo de correo. Dichos procedimientos deben estar vigentes y puestos a disposición de todos los usuarios que los necesiten.	L1	10%
A.12.1.2	Gestión de cambios.	Es necesario controlar los cambios que se lleven a cabo en la institución en cuanto a procesos de negocio, instalaciones de procesamiento de la información y los sistemas que afecten la seguridad de la información.	L2	50%
A.12.1.3	Gestión de capacidades.	Es necesario supervisar y adaptar el uso de los recursos de la institución y realizar proyecciones de los futuros requisitos de capacidad para asegurar el correcto desempeño de las operaciones.	L1	10%
A.12.1.4	Separación de entornos de desarrollo, prueba y producción.	Se requiere para garantizar que los cambios no incorporen nuevos riesgos en los ambientes productivos, y si estos son inevitables que se identifiquen y se realice su oportuno tratamiento.	L1	10%
A.12.2	**Protección contra código malicioso.**			50%
A.12.2.1	Controles contra el código malicioso.	Para el desarrollo de las actividades de la institución se utilizan servicios como Internet, medios extraíbles, los cuales pueden afectar el correcto funcionamiento de activos de información como equipos, software entre otros, por lo tanto es importante establecer controles de seguridad que permitan detección y prevención de la acción de códigos maliciosos así como también procedimientos de concientización de los usuarios.	L2	50%
A.12.3	**Copias de seguridad.**			50%
A.12.3.1	Copias de seguridad de la información.	Se deben manejar esquemas de respaldo de información con el fin de proteger la pérdida de datos y cumplir los requerimientos de disponibilidad para ciertos activos de la entidad.	L2	50%
A.12.4	**Registro de actividad y supervisión.**			20%
A.12.4.1	Registro y gestión de eventos de actividad.	Es necesario configurar auditorias que permitan hacer trazabilidad de actividad, usuario, hora, y máquina con el fin de registrar eventos y generar evidencia.	L1	10%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.12.4.2	Protección de la información de los registros.	Es necesario proteger la información de registro para mantener la integridad de los registros en caso de requerirse una investigación para solucionar un incidente de seguridad o un fallo en los sistemas.	L1	10%
A.12.4.3	Registros de actividad del administrador y operador del sistema.	Es necesario controlar las actividades de los administradores y operadores de los diferentes sistemas de la institución, mediante revisiones regulares a los registros y estos deben protegerse adecuadamente.	L1	10%
A.12.4.4	Sincronización de relojes.	De acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto número 4175 de 2011, el Instituto Nacional de Metrología mantiene, coordina y difunde la hora legal de la República de Colombia. Normativamente todos los equipos de cómputo de las instituciones deben estar sincronizados con la hora legal Colombiana.	L2	50%
A.12.5	**Control del software en explotación.**			50%
A.12.5.1	Instalación del software en sistemas operativos.	Es necesario controlar la instalación de software en los equipos de la institución para asegurar la integridad de los sistemas operacionales	L2	50%
A.12.6	**Gestión de la vulnerabilidad técnica.**			30%
A.12.6.1	Gestión de las vulnerabilidades técnicas.	El ICFES tiene activos de información tecnológicos los cuales están expuestos a vulnerabilidades de tipo técnico, por lo tanto es necesario establecer controles que permitan obtener información acerca de estas vulnerabilidades para ser evaluadas y garantizar la reducción de los riesgos derivados de estas vulnerabilidades técnicas.	L1	10%
A.12.6.2	Restricciones en la instalación de software.	ES necesario establecer reglas para la instalación de software por parte de los usuarios para asegurar la integridad de los sistemas operativos	L2	50%
A.12.7	**Consideraciones de las auditorías de los sistemas de información.**			35%
A.12.7.1	Controles de auditoría de los sistemas de información.	Para minimizar el impacto de las actividades de verificación de los sistemas operativos de los equipos de la institución es necesario planificar y acordar cuidadosamente el desarrollo de estas actividades.	L1	10%
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES.**	**Se comprobara la gestión y la seguridad de las comunicaciones.**		**37%**
A.13.1	**Gestión de la seguridad en las redes.**			63%
A.13.1.1	Controles de redes.	Para proteger la información en las redes de comunicaciones de Méderi, se deben controlar los riesgos asociadas a ellas, segregándolas y limitando los servicios entre ellas.	L2	50%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	Es necesario proteger las redes de Méderi sobre las que se desarrollan todas las aplicaciones ejecutadas por los usuarios, por lo anterior es importante establecer controles de seguridad para asegurar la información en la red, protegerla de amenazas y garantizar su infraestructura de soporte. Establecer la segmentación con base en el nivel de criticidad de los activos. Definición de las direcciones IP origen y destino, puertos para el tráfico autorizado. Establecer control de acceso por puerto en los switches. Implementar un sistema de networkaccess control para establecer una postura de seguridad para los equipos que se conecten a la red. Incluir todas las aplicaciones y servicios de red en el sistema de seguridad de la entidad.	L2	50%
A.13.1.3	Separación de las redes.	Es necesario separar las redes para la protección de su información, especialmente para aislar la red de ítems por su criticidad.	L3	90%
A.13.2	**Intercambio de información con partes externas.**			10%
A.13.2.1	Políticas y procedimientos de transferencia de información.	Dentro del desarrollo normal de las actividades de Méderi se presentan actividades de intercambio de información entre colaboradores, áreas, otras instituciones, entre otros como parte del desarrollo de las actividades, por lo cual es importante establecer políticas y procedimientos que regulen dichas transferencias manteniendo segura la información transferida.	L1	10%
A.13.2.2	Acuerdos de intercambio de información.	Se deben establecer acuerdos para la transferencia de información entre Méderi y terceros. Para garantizar que no se presente uso inadecuado o corrupción cuando la información sale fuera de las instalaciones de la organización.	L1	10%
A.13.2.3	Mensajería electrónica.	Se debe proteger la transferencia de información por mensajería electrónica ya que este es un sistema utilizado por la entidad.	L1	10%
A.13.2.4	Acuerdos de confidencialidad y secreto.	Debido a la importancia de la información que gestiona Méderi es necesario documentar los requisitos específicos para los acuerdos de confidencialidad o no divulgación para proteger dicha información. Estos acuerdos deben ser revisados y actualizados regularmente para que cumplan con las necesidades de la organización.	L2	50%
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**	**Se deben comprobar que se realiza el mantenimiento y el desarrollo de los sistemas según los puntos de control del capítulo.**		**20%**
A.14.1	**Requisitos de seguridad de los sistemas de información.**			37%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información.	Méderi dentro del desarrollo de sus actividades utiliza herramientas ofimáticas, tecnológicas y realiza desarrollos de sistemas de información internamente, en tal sentido es necesario establecer controles de seguridad de la información para garantizar que se protege adecuadamente la información en los nuevos sistemas y/o al surgir cambios en la tecnología de la empresa.	L2	50%
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Es necesario implementar controles de seguridad que ayuden a proteger la información de Méderi de las aplicaciones que pasan sobre redes públicas.	L2	50%
A.14.1.3	Protección de las transacciones por redes telemáticas.	Se deben implementar controles para proteger la información involucrada en las transacciones de las aplicaciones desarrolladas y utilizadas por la institución.	L1	10%
A.14.2	**Seguridad en los procesos de desarrollo y soporte.**			14%
A.14.2.1	Política de desarrollo seguro de software.	La organización para el desarrollo de actividades de los proyectos desarrolla sistemas de información, por lo cual es necesario establecer controles de seguridad para su desarrollo seguro, que permitan garantizar que cumplen con las características técnicas y de seguridad que se requiere.	L1	10%
A.14.2.2	Procedimientos de control de cambios en los sistemas.	Se requiere implementar procedimientos de control de cambios para garantizar que los cambios no incorporen nuevos riesgos en los ambientes productivos, y si estos son inevitables que se identifiquen y se realice su oportuno tratamiento.	L2	50%
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Debido al constante cambio en las plataformas de operación se deben realizar pruebas y revisiones a las aplicaciones críticas de la institución con el fin de asegurar que no haya impactos adversos en la seguridad o en las operaciones.	L1	10%
A.14.2.4	Restricciones a los cambios en los paquetes de software.	Se hace necesario establecer controles de seguridad que garanticen que todos los cambios realizados a los paquetes de software se controlan, revisan y someten a pruebas para no comprometer la seguridad del sistema ni el entorno operativo y también evitar así la fuga de información.	L1	10%
A.14.2.5	Principios de construcción de los sistemas seguros	Debido a que Méderi implementa constantemente diferentes sistemas de información, se deben establecer lineamientos para la construcción de sistemas seguros y exigir que sean cumplidos.	L1	10%
A.14.2.6	Ambiente de desarrollo seguro.	Debido a que Méderi desarrolla sistemas de información se deben establecer ambientes de desarrollo adecuados para brindar los niveles de seguridad adecuados.	L1	10%
A.14.2.7	Desarrollo de software contratado externamente.	Méderi requiere para algunas de las actividades el desarrollo de software contratado externamente, por lo tanto se deben establecer controles de seguridad para proteger el acceso al código fuente de los sistemas de información, para evitar su alteración o uso malintencionado.	L1	10%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Para asegurar que los sistemas desarrollados cumplan con las funcionalidades de seguridad establecidas es necesario realizar pruebas específicas de seguridad.	L1	10%
A.14.2.9	Pruebas de aceptación de sistemas.	Cuando se implementen sistemas de información nuevos u ocurran actualizaciones y nuevas versiones, se requiere establecer criterios de aceptación y establecer programas de pruebas para estos sistemas.	L1	10%
A.14.3	**Datos de prueba.**			10%
A.14.3.1	Protección de los datos utilizados en pruebas.	Méderi utiliza algunos datos para realizar pruebas por ello se debe asegurar la protección de estos datos.	L1	10%
A.15	**RELACIONES CON SUMINISTRADORES.**	**Se comprobará la relación formal con los proveedores.**		**30%**
A.15.1	**Seguridad de la información en las relaciones con proveedores.**			10%
A.15.1.1	Política de seguridad de la información para proveedores.	Debido a que los proveedores del Méderi tienen acceso a diversos activos, es necesario implementar una política que establezca los lineamientos para mitigar los riesgos asociados al acceso a dichos activos.	L1	10%
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	Se deben establecer acuerdos de servicio con los proveedores de la institución que incluyan requisitos de seguridad de la información.	L1	10%
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	Dentro de los acuerdos de servicio que se establezcan con los proveedores de la institución es necesario incluir requisitos de seguridad de la información asociados con la cadena de suministros.	L1	10%
A.15.2	**Gestión de la prestación del servicio por suministradores.**			50%
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	Para garantizar el cumplimiento de los requisitos de seguridad exigidos por Méderi por parte de los proveedores, es necesario realizar el monitoreo y revisión de los servicios prestados a la entidad	L2	50%
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	Cuando surjan cambios en el suministro de servicios por parte de los proveedores, estos cambios deben ser gestionados de acuerdo a la criticidad de la información sistemas y procesos de negocio involucrados.	L2	50%
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**	**Se comprobará el cumplimiento de los puntos de control descritos para la gestión de incidencias.**		**23%**
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras.**			**23%**
A.16.1.1	Responsabilidades y procedimientos.	Para dar una respuesta eficaz a los incidentes de seguridad de la información que se puedan presentar en la institución es necesario establecer las responsabilidades y forma de trabajo ante estos.	L1	10%
A.16.1.2	Notificación de los eventos de seguridad de la información.	Es necesario establecer los canales adecuados para que los eventos de seguridad de Méderi puedan ser reportados tan pronto como sea posible.	L1	10%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.16.1.3	Notificación de puntos débiles de la seguridad	Los colaboradores de Méderi deben estar obligados a reportar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas de información para su gestión.	L2	50%
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Para garantizar la correcta gestión de los eventos de seguridad de la institución estos deben ser evaluados por el personal de seguridad de la información.	L1	10%
A.16.1.5	Respuesta a los incidentes de seguridad.	Es necesario manejar un esquema de respuesta y corrección a los incidentes de seguridad de acuerdo a los procedimientos documentados en la institución.	L1	10%
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	Se debe reducir la posibilidad o impacto de incidentes de seguridad de la información en la institución usando el conocimiento adquirido de la gestión de incidentes pasados.	L1	10%
A.16.1.7	Recopilación de evidencias.	Es necesario construir protocolos de recopilación de evidencia en caso que un incidente de seguridad lo requiera para tratamiento forense.	L1	10%
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**	**Se comprobarán si se cumplen los puntos de control asociados a este capítulo de la ISO 27002 sobre la interrupción de actividades del negocio y la protección de los procesos críticos frente a grandes fallos o desastres.**		**17%**
A.17.1	**Continuidad de la seguridad de la información.**			**23%**
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	La institución debe garantizar la continuidad de la gestión de la seguridad de la información aun en situaciones adversas.	L2	50%
A.17.1.2	Implantación de la continuidad de la seguridad de la información.	Para darle continuidad adecuada a la gestión de la seguridad de la información en situaciones adversas, es necesario establecer, documentar, implementar y mantener procesos, procedimientos y controles de la seguridad de la información.	L1	10%
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la información.	Para verificar que los controles de continuidad de seguridad de la información implementados en la institución son válidos se deben realizar revisiones a intervalos de tiempo regulares.	L1	10%
A.17.2	**Redundancias.**			**10%**
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	Para asegurar la disponibilidad de las instalaciones de procesamiento de información de la institución estas deben contar con redundancia.	L1	10%
A.18	**CUMPLIMIENTO.**	**Se comprobará si se cumplen las normativas vigentes.**		**41%**
A.18.1	**Cumplimiento de los requisitos legales y contractuales.**			58%
A.18.1.1	Identificación de la legislación aplicable.	Es un requerimiento normativo que Méderi cuente con un normograma actualizado que incluya las leyes que debe cumplir.	L2	50%
A.18.1.2	Derechos de propiedad intelectual (DPI).	Para evitar el incumplimiento normativo relacionado con derechos de autor deben implementarse procedimientos apropiados de propiedad intelectual y uso de software patentado.	L3	90%

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Descripción	Valoración	Efectividad
Anexo E. Continuación				
A.18.1.3	Protección de los registros de la organización.	Este control debe implementarse porque hace parte de lo que solicita el Modelo Estándar de Control Interno como COSO o COBIT	L1	10%
A.18.1.4	Protección de datos y privacidad de la información personal.	Este control aplica ya que la entidad está obligada a cumplir con la Ley de Protección de Datos Personales.	L3	90%
A.18.1.5	Regulación de los controles criptográficos.	El uso de control criptográfico como cifrado de contraseñas o cifrado de información sensible en bases de datos o activos de información confidenciales es indispensable para mantener el riesgo operacional dentro de los niveles aceptables.	L2	50%
A.18.2	**Revisiones de la seguridad de la información.**			23%
A.18.2.1	Revisión independiente de la seguridad de la información.	Para asegurar que la seguridad de la información se implementa y opera adecuadamente en el instituto, se deben realizar revisiones al SGSI a intervalos planificados o cuando surjan cabios significativos.	L1	10%
A.18.2.2	Comprobación del cumplimiento	Los directores deben revisar el cumplimiento de los lineamientos de seguridad de sus áreas, para asegurar que la información se opera de acuerdo a estos lineamientos.	L1	10%
A.18.2.3	Disponibilidad de instalaciones para el procesamiento de la información.	Se debe revisar el cumplimiento de los lineamientos de seguridad de los sistemas de información del instituto, para asegurar que la información se opera de acuerdo a estos lineamientos.	L2	50%

Anexo F. Reporte de incidentes Servinte

Este formato se diligenciará para relacionar cada uno de los por menores de un incidente reportado y confirmado así poder establecer las evidenciar y soportes para el adecuado tratamiento del incidente.

Reporte incidente Servinte			
Fecha de incidente		**Ticket Asociado**	
Identificación del Riesgo Asociado			
Describa los riesgos asociados al incidente según analisis de riesgos			
Descripción del incidente			
Describa el incidente presentado			
Procesos Afectados			
Relacione cada uno de los procesos criticos afectados según BIA			
Activos de información afectados			
Relacione cada uno de los activos de información afectados			
Observaciones			
Mencione sus comentarios adicionales del incidente			
Firma Jefe Tecnologia y comunicaciones		**Firma Coordinador de seguridad**	

Anexo G. Reporte restablecimiento de servicio

Mediante este formato se relacionará de manera detallada las actividades, evidencias y resultados que se obtuvieron a través del tratamiento del incidente.

Reporte restablecimiento de servicio Servinte			
Fecha de Inicio		Ticket Asociado	
Fecha de finalización		Fecha diligenciamiento	

Componentes criticos restablecidos
Describa cada uno de los componenetes totalmente restablecidos y normalizados

Medidas adoptadas / Estrategia
Relacione la estartegia establecida y las medidas adoptadas para el restablecimiento del servicio

Procedimientos restablecidos
Relacione cada uno de los procesos criticos restablecidos en su totalidad

Causas / Hallazgos
Relacione cada uno de las causas y hallazgos evaluados durante el restablecimiento del servicio

Lecciones aprendidas
Relacione cada uno de los lecciones aprendidas y oportunidades de mejora identificadas

Observaciones
Mencione sus comentarios adicionales respecto al restablecimiento del servicio

Firma Jefe Tecnologia y comunicaciones		Firma Coordinador de seguridad	
Firma Coodinador de infraestructura		Firma Coordinador de base de datos	
Firma DBA		Firma Ingeniero de base de datos	
Firma Jefe de enfermeria Clinica			

Anexo H. Formato pruebas DRP – Servinte

Para realizar las pruebas definidas y programadas para este plan se diligenciará el siguiente formato, mediante el cual se tendrá un registro y control de los responsables y las actividades a realizar.

Reporte Pruebas DRP - Servinte			
Fecha		Responsable	
Estrategía a probar			

Cronograma				
Defina cada una de las actividades principales en el desarrollo de la prueba(Si existen mas, digitelas)				
N°	Actividad propuesta	Responsable	Hora y fecha inicio	Hora y fecha final
1.	Reunión de inicio			
2.	Recolección de informacion y planeamiento			
3.	identificación de roles y responsabilidades			
4.	Declaración de Inicio de la prueba			
5.	Declaración de finalización de la prueba			
6.	reunión de finalización			
7.	Informe de prueba			

Riesgos Asociados
Relacione los riesgos asociados al eventual indisponibilidad del servicio
1.
2.
3.
4.

Componentes involucrados
Relacione cada uno de los componentes criticos relacionados en la prueba (Activos de información)
1.
2.
3.
4.

Control de cambios			
Relacione clos cambios realizados a los componentes necesarios para la prueba.			
Componente	Cambio realizado	Aprueba	Ejecuta

Equipo de recuperación en la prueba		
Integrantes del equipo de recupracion involucrados en la prueba		
Nombres y apellidos	Cargo	Firma de asistencia

Observadores de la prueba		
Observadores de prueba definidos por dirección del hospital Mederi		
Nombres y apellidos	**Cargo**	**Firma de asistencia**

Actividades a realizar					
Relacione cada una de las actividades a realizar, el responsable, duración y resultado de la misma					
Actividad	**Responsable**	**Fecha y hora de inicio**	**Fecha y hora de finzalización**	**tiempo total**	**Resultado**

Anexos y evidencias		
Relacione cada uno de los anexos que resultaron		
Consecutivo	**Nombre de Anexo**	**Descripción de anexo**

Conclusiones
Mencione las conclusiones y observaciones de la prueba

Firma Jefe Tecnologia y comunicaciones		**Firma Coordinador de seguridad**	
Firma Coodinador de infraestructura		**Firma Coordinador de base de datos**	
Firma DBA		**Firma Ingeniero de base de datos**	
Firma Observador 1		**Firma Observador 2**	

Anexo I. Evaluación de conocimientos

Se define el siguiente formato para el diseño de evaluaciones de conocimiento aplicadas en cada una de las capacitaciones.

Evaluación de conocimientos			
Fecha		**Nombre**	
Tema de capacitación		**Cargo**	
Las siguientes preguntas son de selección múltiple única respuesta, por favor lea detenidamente y marque con una equis (X) la respuesta que crea correcta			
1. Pregunta			
a.	*Primera opción de respuesta*		
b.	*Segunda opción de respuesta*		
c.	*Tercera opción de respuesta*		
d.	*Cuarta opción de respuesta*		
2. Pregunta			
a.	*Primera opción de respuesta*		
b.	*Segunda opción de respuesta*		
c.	*Tercera opción de respuesta*		
d.	*Cuarta opción de respuesta*		
3. Pregunta			
a.	*Primera opción de respuesta*		
b.	*Segunda opción de respuesta*		
c.	*Tercera opción de respuesta*		
d.	*Cuarta opción de respuesta*		
4. Pregunta			
a.	*Primera opción de respuesta*		
b.	*Segunda opción de respuesta*		
c.	*Tercera opción de respuesta*		
d.	*Cuarta opción de respuesta*		

Anexo J. Evaluación al capacitador

Para que el proceso de capacitación y concientización sea objetivo y adquiera mejora continua será necesario que el personal objetivo de capacitación evalué los recursos de la capacitación y al capacitador por medio del siguiente formato.

Evaluación al capacitador					
Fecha		Capacitador			
Tema de capacitación					
Con el objetivo de obtener una mejora continua en nuestro proceso de capacitación, por favor diligencia cada una de los aspectos a continuación consultados					
Marque con equis X la calificación que usted crea de acuerdo al desarrollo de esta capacitación en los ítems mencionados	**Deficiente**	**Aceptable**	**Bueno**	**Muy bueno**	**excelente**
1. Temática de la capacitación					
1.1 Antes de esta capacitación, mi nivel de conocimientos o competencias para el objetivo de este curso era.					
1.2 Después de esta capacitación mi nivel de conocimientos o competencias para el objetivo de este curso era.					
1.3 Seleccione el nivel de importancia del contenido de la capacitación en relación con el DRP .					
1.4 El nivel de profundidad de los contenidos de la capacitación ha sido adecuado.					
1.5 Los objetivos de la capacitación fueron presentados al inicio de la misma y éstos se han cumplido satisfactoriamente.					
2. Competencias del capacitador					
2.1 El capacitador tiene dominio, conocimiento del tema tratado, facilitando el aprendizaje de la audiencia objetivo.					
2.2 El capacitador ha expuesto los temas con claridad.					
2.3 La capacitación está estructurada de modo comprensible, siendo adecuado su contenido teórico y práctico.					
2.4 El capacitador resolvió inquietudes adecuadamente					
2.5 El tiempo utilizado se ajusto a la programación y a la temática tratada.					
3. Aspectos generales					
3.1 El material entregado en la capacitación en la capacitación ha sido útil, adecuado, claro y acorde con los objetivos y contenidos de la misma.					
3.2 Los recursos audiovisuales utilizados fueron óptimos					
3.3 La capacitación inicio y termino según el horario programado					
3.4 La organización logística (Auditorio, audiovisuales, materiales) de la capacitación fue					
3.5 En general como evalúa esta capacitación					
4. Observaciones					